NORMA BRASILEIRA

ABNT NBR ISO/IEC 27002

Primeira edição
31.08.2005

Válida a partir de
30.09.2005

Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação

Information technology – Security technical – Code of pratice for information security management

Palavras-chave: Tecnologia da informação. Segurança.
Descriptors: Information technology. Security.

ICS 35.040

ISBN 978-85-07-00648-0

Número de referência
ABNT NBR ISO/IEC 27002:2005
120 páginas

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretivas ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO/IEC 27002 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:027.00).

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 27002:2005, que foi elaborada pelo Comitê Técnico *Information technology* (ISO/IEC JTC 1), Subcomitê SC 27, *Security techniques*, conforme ISO/IEC Guide 21-1:2005.

Esta primeira edição da ABNT NBR ISO/IEC 27002 compreende a ABNT NBR ISO/IEC 17799:2005 (Versão Corrigida de 02.07.2007) e a Errata 2 de 10.09.2007. Seu conteúdo técnico é idêntico ao da ABNT NBR ISO/IEC 17799:2005 (Versão Corrigida de 02.07.2007). A Errata 2:2007 altera o número de referência da norma de 17799 para 27002. A ABNT NBR ISO/IEC 17799:2005 e a Errata 2:2007 serão provisoriamente mantidas até a publicação da segunda edição da ABNT NBR ISO/IEC 27002.

NORMA BRASILEIRA ABNT NBR ISO/IEC 17799:2005
ERRATA 2
Publicada em 10.09.2007

Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

ERRATA 2

Esta Errata 2 da ABNT NBR ISO/IEC 17799:2005, elaborada pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:027.00), tem por objetivo adotar o Technical Corrigendum 1 da ISO/IEC 17799:2005.

Em todo o documento:

Substituir “17799” por “27002”.

ICS 35.040 **Ref.: ABNT NBR ISO/IEC 17799:2005/Err.2:2007**

NORMA BRASILEIRA

ABNT NBR ISO/IEC 17799

Segunda edição
31.08.2005

Válida a partir de
30.09.2005

Versão corrigida
02.07.2007

Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação

Information technology – Security technical – Code of pratice for information security management

Palavras-chave: Tecnologia da informação. Segurança.
Descriptors: Information technology. Security.

ICS 35.040

ISBN 978-85-07-00519-3

Número de referência
ABNT NBR ISO/IEC 17799:2005
120 páginas

Sumário

Página

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

A ABNT NBR ISO/IEC 17799 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01). O Projeto circulou em Consulta Nacional conforme Edital nº 03, de 31.03.2005, com o número de Projeto NBR ISO/IEC 17799.

Esta Norma é equivalente à ISO/IEC 17799:2005.

Uma família de normas de sistema de gestão de segurança da informação (SGSI) está sendo desenvolvida no ISO/IEC JTC 1/SC 27. A família inclui normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação. Esta família adotará um esquema de numeração usando a série de números 27000 em seqüência.

A partir de 2007, a nova edição da ISO/IEC 17799 será incorporada ao novo esquema de numeração como ISO/IEC 27002.

Os termos relacionados a seguir, com a respectiva descrição, foram mantidos na língua inglesa, por não possuírem tradução equivalente para a língua portuguesa:

Back-up – cópias de segurança de arquivos.

BBS (*Bulletin Board System*) – sistema no qual um computador pode se comunicar com outros computadores por meio de linha telefônica, como na *Internet*.

Buffer overflow/overrun – transbordamento de dados. Situação que ocorre quando dados em demasia são aceitos na entrada de uma aplicação ou durante o processamento interno do sistema, ultrapassando a sua capacidade de armazenamento.

Call back – retorno de chamada.

Call center – central de atendimento.

Call forwarding – encaminhamento de chamada.

Covert channel – canal de comunicações que permite o fluxo de informações de uma maneira que viole a política de segurança do sistema.

Denial of service (negação do serviço) – impedimento do acesso autorizado aos recursos ou retardamento de operações críticas por um certo período de tempo.

Dial up – serviço por meio do qual um computador pode usar a linha telefônica para iniciar e efetuar uma comunicação com outro computador.

Display – dispositivo de apresentação de dados.

Download – descarregamento, transferência de arquivos entre computadores por meio de uma rede.

E-business – modalidade eletrônica de realização de transações de negócios.

EDI – Eletronic Data Interchange – intercâmbio eletrônico de dados.

E-government – modalidade eletrônica de realização de transações de negócios e prestação de serviços por entidades governamentais.

Firewall – sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes.

Flash Disks – dispositivos de armazenamento de dados que utiliza circuitos integrados de memória não volátil.

Gateway – equipamento que funciona como ponto de conexão entre duas redes.

Hacker – pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat*.

Hash – representação matemática única de um conjunto de dados (resumo de mensagem).

Help desk – fonte de suporte técnico aos usuários.

ISP – provedores de serviços de *Internet*.

Log-On – processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema.

Logging – registro do histórico de atividades realizadas ou de eventos ocorridos em um determinado sistema ou processo.

Middleware – personalização de *software*; *software* de sistema que foi personalizado por um vendedor para um usuário particular.

Need to know – conceito que define que uma só pessoa precisa acessar os sistemas necessários para realizar a sua atividade.

Network worms (vermes de rede) – código malicioso autopropagável que pode ser distribuído automaticamente de um computador para outro por meio de conexões de rede local ou pela *Internet*. Um *worm* pode realizar ações perigosas, como consumir banda de rede e recursos locais.

Patch – correção temporária efetuada em um programa; pequena correção executada pelo usuário no *software*, com as instruções do fabricante do *software*.

PDA – assistente digital pessoal.

PIN (*Personal Identification Number*) – número de identificação pessoal.

Program-to-program controls – controles entre programas.

Root – usuário administrador com privilégios irrestritos no sistema.

Run-to-run controls – controles entre execuções.

Scanners – periférico de digitalização de imagens e documentos.

Snapshot – retrato do estado de um sistema em um estágio específico.

Sniffer – um *software* ou dispositivo especializado que captura pacotes na rede.

Timestamp (carimbo de tempo) – registro temporal de um evento.

Tokens – Dispositivo físico para autenticação. Exemplos: *token* criptográfico, *token* de senha dinâmica, *token* de memória, entre outros.

UTC – *Coordinated Universal Time* – Tempo Universal Coordenado.

Wireless – sistema de comunicação que não requer fios para transportar sinais.

Em 6.1.3, Diretrizes para implementação, primeiro parágrafo, a ISO/IEC 17799:2005 faz uma referência equivocada à seção 4. Esse equívoco foi corrigido nesta ABNT NBR ISO/IEC 17799 e a notificação deste foi feita ao ISO/IEC JTC 1 para correção da norma original.

Esta segunda edição cancela e substitui a edição anterior (ABNT NBR ISO/IEC 17799:2001), a qual foi tecnicamente revisada.

Esta versão corrigida da ABNT NBR ISO/IEC 17799:2005 incorpora a Errata 1 de 28.08.2006 e Errata 1 de 02.07.2207.

0 Introdução

0.1 O que é segurança da informação?

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ver OECD Diretrizes para a Segurança de Sistemas de Informações e Redes).

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software e hardware.* Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

0.2 Por que a segurança da informação é necessária?

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes ou outras partes externas. Uma consultoria externa especializada pode ser também necessária.

0.3 Como estabelecer requisitos de segurança da informação

É essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação.

1. Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.

2. Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

0.4 Analisando/avaliando os riscos de segurança da informação

Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos.

Convém que a análise/avaliação de riscos seja repetida periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação.

Informações adicionais sobre a análise/avaliação de riscos de segurança da informação podem ser encontradas em 4.1 "Analisando/avaliando os riscos de segurança da informação".

0.5 Seleção de controles

Uma vez que os requisitos de segurança da informação e os riscos tenham sido identificados e as decisões para o tratamento dos riscos tenham sido tomadas, convém que controles apropriados sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta Norma ou de um outro conjunto de controles ou novos controles podem ser desenvolvidos para atender às necessidades específicas, conforme apropriado. A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes.

Alguns dos controles nesta Norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações. Estes controles são explicados em mais detalhes no item "Ponto de partida para a segurança da informação".

Informações adicionais sobre seleção de controles e outras opções para tratamento de risco podem ser encontradas em 4.2 "Tratamento dos riscos de segurança da informação".

0.6 Ponto de partida para a segurança da informação

Um certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação. Estes controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) proteção de dados e privacidade de informações pessoais (ver 15.1.4);

b) proteção de registros organizacionais (ver 15.1.3);

c) direitos de propriedade intelectual (ver 15.1.2).

Os controles considerados práticas para a segurança da informação incluem:

a) documento da política de segurança da informação (ver 5.1.1);

b) atribuição de responsabilidades para a segurança da informação (ver 6.1.3);

c) conscientização, educação e treinamento em segurança da informação (ver 8.2.2);

d) processamento correto nas aplicações (ver 12.2);

e) gestão de vulnerabilidades técnicas (ver 12.6);

f) gestão da continuidade do negócio (ver seção 14);

g) gestão de incidentes de segurança da informação e melhorias (ver 13.2).

Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes.

Convém observar que, embora todos os controles nesta Norma sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. Por isto, embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos.

0.7 Fatores críticos de sucesso

A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

b) uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível de todos os níveis gerenciais;

d) um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

e) divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

g) provisão de recursos financeiros para as atividades da gestão de segurança da informação;

h) provisão de conscientização, treinamento e educação adequados;

i) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

j) implementação de um sistema de medição[1], que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

0.8 Desenvolvendo suas próprias diretrizes

Esta Norma pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para a organização. Nem todos os controles e diretrizes contidos nesta Norma podem ser aplicados. Além disto, controles adicionais e recomendações não incluídos nesta Norma podem ser necessários. Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma referência cruzada para as seções desta Norma, onde aplicável, para facilitar a verificação da conformidade por auditores e parceiros do negócio.

[1] Deve-se observar que as medições de segurança da informação estão fora do escopo desta Norma.

Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação

1 Objetivo

Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais.

2 Termos e definições

Para os efeitos desta Norma, aplicam-se os seguintes termos e definições.

2.1
ativo
qualquer coisa que tenha valor para a organização
[ISO/IEC 13335-1:2004]

2.2
controle
forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal
NOTA Controle é também usado como um sinônimo para proteção ou contramedida.

2.3
diretriz
descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas
[ISO/IEC 13335-1:2004]

2.4
recursos de processamento da informação
qualquer sistema de processamento da informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem

2.5
segurança da informação
preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas

2.6
evento de segurança da informação
ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação
[ISO/IEC TR 18044:2004]

2.7
incidente de segurança da informação
um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
[ISO/IEC TR 18044:2004]

2.8
política
intenções e diretrizes globais formalmente expressas pela direção

2.9 risco
combinação da probabilidade de um evento e de suas conseqüências
[ABNT ISO/IEC Guia 73:2005]

2.10
análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco
[ABNT ISO/IEC Guia 73:2005]

2.11
análise/avaliação de riscos
processo completo de análise e avaliação de riscos
[ABNT ISO/IEC Guia 73:2005]

2.12
avaliação de riscos
processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco
[ABNT ISO/IEC Guia 73:2005]

2.13
gestão de riscos
atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos
NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.
[ABNT ISO/IEC Guia 73:2005]

2.14
tratamento do risco
processo de seleção e implementação de medidas para modificar um risco
[ABNT ISO/IEC Guia 73:2005]

2.15
terceira parte
pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto
[ABNT ISO/IEC Guia 2:1998]

2.16
ameaça
causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO/IEC 13335-1:2004]

2.17
vulnerabildade
fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças

3 Estrutura desta Norma

Esta Norma contém 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos.

3.1 Seções

Cada seção contém um número de categorias principais de segurança da informação. As 11 seções (acompanhadas com o respectivo número de categorias) são:

a) Política de Segurança da Informação (1);

b) Organizando a Segurança da Informação (2);

c) Gestão de Ativos (2);

d) Segurança em Recursos Humanos (3);

e) Segurança Física e do Ambiente (2);

f) Gestão das Operações e Comunicações (10);

g) Controle de Acesso (7);

h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6);

i) Gestão de Incidentes de Segurança da Informação (2);

j) Gestão da Continuidade do Negócio (1);

k) Conformidade (3).

Nota: A ordem das seções nesta Norma não significa o seu grau de importância. Dependendo das circunstâncias, todas as seções podem ser importantes. Portanto, convém que cada organização que utilize esta Norma identifique quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio. Todas as alíneas nesta Norma também não estão ordenadas por prioridade, a menos que explicitado.

3.2 Principais categorias de segurança da informação

Cada categoria principal de segurança da informação contém:

a) um objetivo de controle que define o que deve ser alcançado; e

b) um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

As descrições dos controles estão estruturadas da seguinte forma:

<u>Controle</u>
Define qual o controle específico para atender ao objetivo do controle.

<u>Diretrizes para a implementação</u>
Contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas.

Informações adicionais
Contém informações adicionais que podem ser consideradas, como, por exemplo, considerações legais e referências a outras normas.

4 Análise/avaliação e tratamento de riscos

4.1 Analisando/avaliando os riscos de segurança da informação

Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos. O processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos.

Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).

Convém que as análises/avaliações de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando uma mudança significativa ocorrer. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário.

O escopo de uma análise/avaliação de riscos pode tanto ser em toda a organização, partes da organização, em um sistema de informação específico, em componentes de um sistema específico ou em serviços onde isto seja praticável, realístico e útil. Exemplos de metodologias de análise/avaliação de riscos são discutidas no ISO/IEC TR 13335-3 (*Guidelines for the management of IT security: Techniques for the management of IT Security*).

4.2 Tratando os riscos de segurança da informação

Convém que, antes de considerar o tratamento de um risco, a organização defina os critérios para determinar se os riscos podem ser ou não aceitos. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a organização. Convém que tais decisões sejam registradas.

Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do risco, incluem:

a) aplicar controles apropriados para reduzir os riscos;

b) conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação de risco;

c) evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;

d) transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Convém que, para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

a) os requisitos e restrições de legislações e regulamentações nacionais e internacionais;

b) os objetivos organizacionais;

c) os requisitos e restrições operacionais;

d) custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização;

e) a necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Os controles podem ser selecionados desta Norma ou de outros conjuntos de controles, ou novos controles podem ser considerados para atender às necessidades específicas da organização. É importante reconhecer que alguns controles podem não ser aplicáveis a todos os sistemas de informação ou ambientes, e podem não ser praticáveis para todas as organizações. Como um exemplo, 10.1.3 descreve como as responsabilidades podem ser segregadas para evitar fraudes e erros. Pode não ser possível para pequenas organizações segregar todas as responsabilidades e, portanto, outras formas de atender o mesmo objetivo de controle podem ser necessárias. Em um outro exemplo, 10.10 descreve como o uso do sistema pode ser monitorado e as evidências coletadas. Os controles descritos, como, por exemplo, eventos de *"logging"*, podem conflitar com a legislação aplicável, tais como a proteção à privacidade dos clientes ou a exercida nos locais de trabalho.

Convém que os controles de segurança da informação sejam considerados na especificação dos requisitos e nos estágios iniciais dos projetos e sistemas. Caso isso não seja realizado, pode acarretar custos adicionais e soluções menos efetivas, ou mesmo, no pior caso, incapacidade de se alcançar a segurança necessária.

Convém que seja lembrado que nenhum conjunto de controles pode conseguir a segurança completa, e que uma ação gerencial adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, para apoiar as metas da organização.

5 Política de segurança da informação

5.1 Política de segurança da informação

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

Convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

5.1.1 Documento da política de segurança da informação

Controle
Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Diretrizes para implementação
Convém que o documento da política de segurança da informação declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação. Convém que o documento da política contenha declarações relativas a:

a) uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação (ver introdução);

b) uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;

c) uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;

d) breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:

   1) conformidade com a legislação e com requisitos regulamentares e contratuais;

   2) requisitos de conscientização, treinamento e educação em segurança da informação;

   3) gestão da continuidade do negócio;

   4) conseqüências das violações na política de segurança da informação;

e) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;

f) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

Convém que esta política de segurança da informação seja comunicada através de toda a organização para os usuários de forma que seja relevante, acessível e compreensível para o leitor em foco.

Informações adicionais
A política de segurança da informação pode ser uma parte de um documento da política geral. Se a política de segurança da informação for distribuída fora da organização, convém que sejam tomados cuidados para não revelar informações sensíveis. Informações adicionais podem ser encontradas na ISO/IEC 13335-1:2004.

5.1.2 Análise crítica da política de segurança da informação

Controle
Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação
Convém que a política de segurança da informação tenha um gestor que tenha responsabilidade de gestão aprovada para desenvolvimento, análise crítica e avaliação da política de segurança da informação. Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança da informação da organização e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente técnico.

Convém que a análise crítica da política de segurança da informação leve em consideração os resultados da análise crítica pela direção. Convém que sejam definidos procedimentos para análise crítica pela direção, incluindo uma programação ou um período para a análise crítica.

Convém que as entradas para a análise crítica pela direção incluam informações sobre:

a) realimentação das partes interessadas;

b) resultados de análises críticas independentes (ver 6.1.8);

c) situação de ações preventivas e corretivas (ver 6.1.8 e 15.2.1);

d) resultados de análises críticas anteriores feitas pela direção;

e) desempenho do processo e conformidade com a política de segurança da informação;

f) mudanças que possam afetar o enfoque da organização para gerenciar a segurança da informação, incluindo mudanças no ambiente organizacional, nas circunstâncias do negócio, na disponibilidade dos recursos, nas questões contratuais, regulamentares e de aspectos legais ou no ambiente técnico;

g) tendências relacionadas com as ameaças e vulnerabilidades;

h) relato sobre incidentes de segurança da informação (ver 13.1);

i) recomendações fornecidas por autoridades relevantes (ver 6.1.6).

Convém que as saídas da análise crítica pela direção incluam quaisquer decisões e ações relacionadas a:

a) melhoria do enfoque da organização para gerenciar a segurança da informação e seus processos;

b) melhoria dos controles e dos objetivos de controles;

c) melhoria na alocação de recursos e/ou de responsabilidades.

Convém que um registro da análise crítica pela direção seja mantido.

Convém que a aprovação pela direção da política de segurança da informação revisada seja obtida.

6 Organizando a segurança da informação

6.1 Organização interna

Objetivo: Gerenciar a segurança da informação dentro da organização.

Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

Convém que a direção aprove a política de segurança da informação, atribua as funções da segurança, coordene e analise criticamente a implementação da segurança da informação por toda a organização.

Se necessário, convém que uma consultoria especializada em segurança da informação seja estabelecida e disponibilizada dentro da organização. Convém que contatos com especialistas ou grupos de segurança da informação externos, incluindo autoridades relevantes, sejam feitos para se manter atualizado com as tendências de mercado, monitorar normas e métodos de avaliação, além de fornecer apoio adequado, quando estiver tratando de incidentes de segurança da informação. Convém que um enfoque multidisciplinar na segurança da informação seja incentivado.

6.1.1 Comprometimento da direção com a segurança da informação

Controle
Convém que a direção apóie ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.

Diretrizes para implementação
Convém que a direção:

a) assegure que as metas de segurança da informação estão identificadas, atendem aos requisitos da organização e estão integradas nos processos relevantes;

b) formule, analise criticamente e aprove a política de segurança da informação;

c) analise criticamente a eficácia da implementação da política de segurança da informação;

d) forneça um claro direcionamento e apoio para as iniciativas de segurança da informação;

e) forneça os recursos necessários para a segurança da informação;

f) aprove as atribuições de tarefas e responsabilidades específicas para a segurança da informação por toda a organização;

g) inicie planos e programas para manter a conscientização da segurança da informação;

h) assegure que a implementação dos controles de segurança da informação tem uma coordenação e permeia a organização (ver 6.1.2).

Convém que a direção identifique as necessidades para a consultoria de um especialista interno ou externo em segurança da informação, analise criticamente e coordene os resultados desta consultoria por toda a organização.

Dependendo do tamanho da organização, tais responsabilidades podem ser conduzidas por um fórum de gestão exclusivo ou por um fórum de gestão existente, a exemplo do conselho de diretores.

Informações adicionais
Outras informações podem ser obtidas na ISO/IEC 13335-1:2004.

6.1.2 Coordenação da segurança da informação

Controle
Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.

Diretrizes para implementação
Convém que a coordenação da segurança da informação envolva a cooperação e colaboração de gerentes, usuários, administradores, desenvolvedores, auditores, pessoal de segurança e especialistas com habilidades nas áreas de seguro, questões legais, recursos humanos, TI e gestão de riscos.

Convém que esta atividade:

a) garanta que as atividades de segurança da informação são executadas em conformidade com a política de segurança da informação;

b) identifique como conduzir as não-conformidades;

c) aprove as metodologias e processos para a segurança da informação, tais como análise/avaliação de riscos e classificação da informação;

d) identifique as ameaças significativas e a exposição da informação e dos recursos de processamento da informação às ameaças;

e) avalie a adequação e coordene a implementação de controles de segurança da informação;

f) promova, de forma eficaz, a educação, o treinamento e a conscientização pela segurança da informação por toda a organização;

g) avalie as informações recebidas do monitoramento e da análise crítica dos incidentes de segurança da informação, e recomende ações apropriadas como resposta para os incidentes de segurança da informação identificados.

Se a organização não usa representantes das diferentes áreas, por exemplo, porque tal grupo não é apropriado para o tamanho da organização, convém que as ações descritas acima sejam conduzidas por um organismo de gestão adequado ou por um gestor individual.

6.1.3 Atribuição de responsabilidades para a segurança da informação

Controle
Convém que todas as responsabilidades pela segurança da informação, estejam claramente definidas.

Diretrizes para implementação
Convém que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com a política de segurança da informação (ver seção 5). Convém que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos sejam claramente definidas. Convém que esta responsabilidade seja complementada, onde for necessário, com orientações mais detalhadas para locais específicos e recursos de processamento de informações. Convém que sejam claramente definidas as responsabilidades em cada local para a proteção dos ativos e para realizar processos de segurança da informação específicos, como, por exemplo, o plano de continuidade de negócios.

Pessoas com responsabilidades definidas pela segurança da informação podem delegar as tarefas de segurança da informação para outros usuários. Todavia eles continuam responsáveis e convém que verifiquem se as tarefas delegadas estão sendo executadas corretamente.

Convém que as áreas pelas quais as pessoas sejam responsáveis, estejam claramente definidas; em particular convém que os seguintes itens sejam cumpridos:

a) os ativos e os processos de segurança da informação associados com cada sistema sejam identificados e claramente definidos;

b) gestor responsável por cada ativo ou processo de segurança da informação tenha atribuições definidas e os detalhes dessa responsabilidade sejam documentados (ver 7.1.2);

c) os níveis de autorização sejam claramente definidos e documentados.

Informações adicionais
Em muitas organizações um gestor de segurança da informação pode ser indicado para assumir a responsabilidade global pelo desenvolvimento e implementação da segurança da informação e para apoiar a identificação de controles.

Entretanto, a responsabilidade pela obtenção dos recursos e implementação dos controles permanece sempre com os gestores. Uma prática comum é indicar um responsável por cada ativo, tornando-o assim responsável por sua proteção no dia a dia.

6.1.4 Processo de autorização para os recursos de processamento da informação

Controle
Convém que seja definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.

Diretrizes para implementação
Convém que as seguintes diretrizes sejam consideradas no processo de autorização:

a) os novos recursos tenham a autorização adequada por parte da administração de usuários, autorizando seus propósitos e uso. Convém que a autorização também seja obtida junto ao gestor responsável pela manutenção do sistema de segurança da informação, para garantir que todas as políticas e requisitos de segurança relevantes sejam atendidos;

b) *hardware* e o *software* sejam verificados para garantir que são compatíveis com outros componentes do sistema, onde necessários;

c) uso de recursos de processamento de informação, pessoais ou privados, como, por exemplo, *note books,* computadores pessoais ou dispositivos do tipo *palm top*, para processamento das informações do negócio, possa introduzir novas vulnerabilidades, e convém que controles necessários sejam identificados e implementados.

6.1.5 Acordos de confidencialidade

Controle
Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular.

Diretrizes para implementação
Convém que os acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal. Para identificar os requisitos para os acordos de confidencialidade ou de não divulgação, convém que sejam considerados os seguintes elementos:

a) uma definição da informação a ser protegida (por exemplo, informação confidencial);

b) tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;

c) ações requeridas quando um acordo está encerrado;

d) responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação (como o conceito "*need to know*");

e) proprietário da informação, segredos comerciais e de propriedade intelectual, e como isto se relaciona com a proteção da informação confidencial;

f) uso permitido da informação confidencial e os direitos do signatário para usar a informação;

g) direito de auditar e monitorar as atividades que envolvem as informações confidenciais;

h) processo para notificação e relato de divulgação não autorizada ou violação das informações confidenciais;

i) termos para a informação ser retornada ou destruída quando do término do acordo; e

j) ações esperadas a serem tomadas no caso de uma violação deste acordo.

Com base nos requisitos de segurança da informação da organização, outros elementos podem ser necessários em um acordo de confidencialidade ou de não divulgação.

Convém que os acordos de confidencialidade e de não divulgação estejam em conformidade com todas as leis e regulamentações aplicáveis na jurisdição para a qual eles se aplicam (ver 15.1.1)

Convém que os requisitos para os acordos de confidencialidade e de não divulgação sejam analisados criticamente de forma periódica e quando mudanças ocorrerem que influenciem estes requisitos.

Informações adicionais
Acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada.

Pode haver a necessidade de uma organização usar diferentes formas de acordos de confidencialidade ou de não divulgação, em diferentes circunstâncias.

6.1.6 Contato com autoridades

Controle
Convém que contatos apropriados com autoridades pertinentes sejam mantidos.

Diretrizes para implementação
Convém que as organizações tenham procedimentos em funcionamento que especifiquem quando e por quais autoridades (por exemplo, obrigações legais, corpo de bombeiros, autoridades fiscalizadoras) devem ser contatadas e como os incidentes de segurança da informação identificados devem ser notificados em tempo hábil, no caso de suspeita de que a lei foi violada.

Organizações que estejam sob ataque da internet podem precisar do apoio de partes externas à organização (por exemplo, um provedor de serviço da internet ou um operador de telecomunicações), para tomar ações contra a origem do ataque.

Informações adicionais
A manutenção de tais contatos pode ser um requisito para apoiar a gestão de incidentes de segurança da informação (ver 13.2) ou da continuidade dos negócios e do processo de planejamento da contingência (ver seção 14). Contatos com organismos reguladores são também úteis para antecipar e preparar para as mudanças futuras na lei ou nos regulamentos, os quais têm que ser seguidos pela organização. Contatos com outras autoridades incluem utilidades, serviços de emergência, saúde e segurança, por exemplo corpo de bombeiros (em conjunto com a continuidade do negócio), provedores de telecomunicação (em conjunto com as rotas de linha e disponibilidade), fornecedor de água (em conjunto com as instalações de refrigeração para os equipamentos).

6.1.7 Contato com grupos especiais

Controle
Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais.

Diretrizes para implementação
Convém que associação a grupos de interesses especiais ou fóruns seja considerada como forma de:

a) ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;

b) assegurar que o entendimento do ambiente de segurança da informação está atual e completo;

c) receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades;

d) conseguir acesso à consultoria especializada em segurança da informação;

e) compartilhar e trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades;

f) prover relacionamentos adequados quando tratar com incidentes de segurança da informação (ver 13.2.1).

Informações adicionais
Acordos de compartilhamento de informações podem ser estabelecidos para melhorar a cooperação e coordenação de assuntos de segurança da informação. Convém que tais acordos identifiquem requisitos para a proteção de informações sensíveis.

6.1.8 Análise crítica independente de segurança da informação

Controle
Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

Diretrizes para implementação
Convém que a análise crítica independente seja iniciada pela direção. Tal análise crítica independente é necessária para assegurar a contínua pertinência, adequação e eficácia do enfoque da organização para gerenciar a segurança da informação. Convém que a análise crítica inclua a avaliação de oportunidades para a melhoria e a necessidade de mudanças para o enfoque da segurança da informação, incluindo a política e os objetivos de controle.

Convém que a análise crítica seja executada por pessoas independentes da área avaliada, como, por exemplo, uma função de auditoria interna, um gerente independente ou uma organização de terceira parte especializada em tais análises críticas. Convém que as pessoas que realizem estas análises críticas possuam habilidade e experiência apropriadas.

Convém que os resultados da análise crítica independente sejam registrados e relatados para a direção que iniciou a análise crítica. Estes registros devem ser mantidos.

Se a análise crítica independente identificar que o enfoque da organização e a implementação para gerenciar a segurança da informação são inadequados ou não-conformes com as orientações estabelecidas para segurança da informação, no documento da política de segurança da informação (ver 5.1.1), convém que a direção considere a tomada de ações corretivas.

Informações adicionais
Convém que as áreas onde os gerentes regularmente fazem a análise crítica (ver 15.2.1) possam também ser analisadas criticamente de forma independente. Técnicas para a análise crítica podem incluir entrevistas com a gerência, verificação de registros ou análise crítica dos documentos da política de segurança da informação. A ABNT NBR ISO 19011:2002, Diretrizes para auditoria de sistemas de gestão da qualidade e/ou do meio ambiente, pode também fornecer orientações para se realizar a análise crítica independente, incluindo o estabelecimento e a implementação de um programa de análise crítica. A subseção 15.3 especifica os controles relevantes para a análise crítica independente de sistemas de informações operacionais e o uso de ferramentas de auditoria de sistemas.

6.2 Partes externas

Objetivo: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.

Convém que a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou serviços oriundos de partes externas.

Convém que qualquer acesso aos recursos de processamento da informação da organização e ao processamento e comunicação da informação por partes externas seja controlado.

Convém que seja feita uma análise/avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários, onde existir uma necessidade de negócio para trabalhar com partes externas, que possa requerer acesso aos recursos de processamento da informação e à informação da organização, ou na obtenção e fornecimento de um produto e serviço de uma parte externa ou para ela. Convém que os controles sejam acordados e definidos por meio de um acordo com a parte externa.

6.2.1 Identificação dos riscos relacionados com partes externas

Controle
Convém que os riscos para os recursos de processamento da informação e da informação da organização oriundos de processos do negócio que envolva as partes externas sejam identificados e controles apropriados implementados antes de se conceder o acesso.

Diretrizes para implementação
Convém que uma análise/avaliação de riscos (ver seção 4) seja feita para identificar quaisquer requisitos de controles específicos, onde existir uma necessidade que permita o acesso de uma parte externa aos recursos de processamento da informação ou à informação de uma organização. Convém que a identificação de riscos relativos ao acesso da parte externa leve em consideração os seguintes aspectos:

a) os recursos de processamento da informação que uma parte externa esteja autorizada a acessar;

b) tipo de acesso que a parte externa terá aos recursos de processamento da informação e à informação, como, por exemplo:

   1) acesso físico ao escritório, sala dos computadores, arquivos de papéis;

   2) acesso lógico ao banco de dados da organização e aos sistemas de informações;

   3) rede de conexão entre a organização e a rede da parte externa, como, por exemplo, conexão permanente, acesso remoto;

   4) se o acesso vai ser dentro ou fora da organização;

c) valor e a sensibilidade da informação envolvida, e a sua criticidade para as operações do negócio;

d) os controles necessários para proteger a informação que não deva ser acessada pelas partes externas;

e) as pessoas das partes externas envolvidas no manuseio das informações da organização;

f) como a organização ou o pessoal autorizado a ter acesso pode ser identificado, como a autorização é verificada e com qual freqüência isto precisa ser reconfirmado;

g) as diferentes formas e controles empregados pela parte externa quando estiver armazenando, processando, comunicando, compartilhando e repassando informações;

h) impacto do acesso não estar disponível para a parte externa, quando requerido, e a entrada ou o recebimento incorreto ou por engano da informação;

i) práticas e procedimentos para tratar com incidentes de segurança da informação e danos potenciais, e os termos e condições para que a parte externa continue acessando, no caso que ocorra um incidente de segurança da informação;

j) que os requisitos legais e regulamentares e outras obrigações contratuais relevantes para a parte externa sejam levados em consideração;

k) como os interesses de quaisquer uma das partes interessadas podem ser afetados pelos acordos.

Convém que o acesso às informações da organização pelas partes externas não seja fornecido até que os controles apropriados tenham sido implementados e, onde for viável, um contrato tenha sido assinado definindo os termos e condições para a conexão ou o acesso e os preparativos para o trabalho. Convém que, de uma forma geral, todos os requisitos de segurança da informação resultantes do trabalho com partes externas ou controles internos estejam refletidos por um acordo com a parte externa (ver 6.2.2 e 6.2.3).

Convém que seja assegurado que a parte externa está consciente de suas obrigações, e aceita as responsabilidades e obrigações envolvendo o acesso, processamento, comunicação ou o gerenciamento dos recursos do processamento da informação e da informação da organização.

Informações adicionais
A informação pode ser colocada em risco por partes externas com uma gestão inadequada da segurança da informação. Convém que os controles sejam identificados e aplicados para administrar o acesso da parte externa aos recursos de processamento da informação. Por exemplo, se existir uma necessidade especial para a confidencialidade da informação, acordos de não divulgação devem ser usados.

As organizações podem estar sujeitas a riscos associados com processos interorganizacionais, gerenciamento e comunicação, se um alto grau de terceirização for realizado, ou onde existirem várias partes externas envolvidas.

Os controles de 6.2.2 e 6.2.3 cobrem diferentes situações para as partes externas, incluindo, por exemplo:

a) provedores de serviço, tais como *ISP*, provedores de rede, serviços de telefonia e serviços de apoio e manutenção;

b) terceirização de operações e recursos, como, por exemplo, sistemas de TI, serviços de coleta de dados, operação de central de atendimento (*call center)*;

c) clientes;

d) operações e/ou recursos de terceirização, como, por exemplo, sistemas de TI, serviços de coleta de dados, operação de *call center*;

e) consultores em negócios e em gestão, e auditores;

f) desenvolvedores e fornecedores, como, por exemplo, de produtos de *software* e sistemas de TI;

g) pessoal de limpeza, serviços de bufês e outros serviços de apoio terceirizados;

h) pessoal temporário, estagiário e outras contratações de curta duração.

Tais acordos podem ajudar a reduzir o risco associado com as partes externas.

6.2.2 Identificando a segurança da informação, quando tratando com os clientes

Controle
Convém que todos os requisitos de segurança da informação identificados sejam considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.

Diretrizes para implementação
Convém que os seguintes termos sejam considerados para contemplar a segurança da informação antes de conceder aos clientes o acesso a quaisquer ativos da organização (dependendo do tipo e extensão do acesso concedido, nem todos os itens são aplicáveis):

a) proteção dos ativos, incluindo:

   1) procedimentos para proteger os ativos da organização, incluindo informação e *software*, e a gestão de vulnerabilidades conhecidas;

   2) procedimentos para determinar se ocorreu qualquer comprometimento de ativos, por exemplo, perda ou modificação de dados;"

   3) integridade;

   4) restrições em relação a cópias e divulgação de informações;

b) descrição do produto ou serviço a ser fornecido;

c) as diferentes razões, requisitos e benefícios para o acesso do cliente;

d) políticas de controle de acesso, cobrindo:

   1) métodos de acesso permitido e o controle e uso de identificadores únicos, tais como identificador de usuário e senhas de acesso;

   2) um processo de autorização para acesso dos usuários e privilégios;

3) uma declaração de que todo o acesso que não seja explicitamente autorizado é proibido;

4) um processo para revogar os direitos de acesso ou interromper a conexão entre sistemas;

e) procedimentos para relato, notificação e investigação de informações imprecisas (por exemplo, sobre pessoal), incidentes de segurança da informação e violação da segurança da informação;

f) descrição de cada serviço que deve estar disponível;

g) os níveis de serviços acordados e os níveis de serviços inaceitáveis;

h) direito de monitorar e revogar qualquer atividade relacionada com os ativos da organização;

i) as respectivas responsabilidades legais da organização e dos clientes;

j) responsabilidades com relação a aspectos legais e como é assegurado que os requisitos legais são atendidos, por exemplo, leis de proteção de dados, especialmente levando-se em consideração os diferentes sistemas legais nacionais se o acordo envolver a cooperação com clientes em outros países (ver 15.1);

k) direitos de propriedade intelectual e direitos autorais (ver 15.1.2) e proteção de qualquer trabalho colaborativo (ver 6.1.5).

Informações adicionais
Os requisitos de segurança da informação relacionados com o acesso dos clientes aos ativos da organização podem variar consideravelmente, dependendo dos recursos de processamento da informação e das informações que estão sendo acessadas. Estes requisitos de segurança da informação podem ser contemplados, usando-se os acordos com o cliente, os quais contêm todos os riscos identificados e os requisitos de segurança da informação (ver 6.2.1).

Acordos com partes externas podem também envolver outras partes. Convém que os acordos que concedam o acesso a partes externas incluam permissão para designação de outras partes elegíveis e condições para os seus acessos e envolvimento.

6.2.3 Identificando segurança da informação nos acordos com terceiros

Controle
Convém que os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação cubram todos os requisitos de segurança da informação relevantes.

Diretrizes para implementação
Convém que o acordo assegure que não existe mal-entendido entre a organização e o terceiro. Convém que as organizações considerem a possibilidade de indenização do terceiro.

Convém que os seguintes termos sejam considerados para inclusão no acordo, com o objetivo de atender aos requisitos de segurança da informação identificados (ver 6.2.1):

a) política de segurança da informação;

b) controles para assegurar a proteção do ativo, incluindo:

1) procedimentos para proteger os ativos da organização, incluindo informação, *software* e *hardware*;

2) quaisquer mecanismos e controles para a proteção física requerida;

3) controles para assegurar proteção contra *software* malicioso (ver 10.4.1);

4) procedimentos para determinar se ocorreu qualquer comprometimento de ativos, por exemplo, perda ou modificação de dados, *software* e *hardware*;

5) controles para assegurar o retorno ou a destruição da informação e dos ativos no final do contrato, ou em um dado momento definido no acordo.

6) confidencialidade, integridade, disponibilidade e qualquer outra propriedade relevante (ver 2.1.5) dos ativos;

7) restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade (ver 6.1.5).

c) treinamento dos usuários e administradores nos métodos, procedimentos e segurança da informação;

d) assegurar a conscientização dos usuários nas questões e responsabilidades pela segurança da informação;

f) provisão para a transferência de pessoal, onde necessário;

f) responsabilidades com relação à manutenção e instalação de *software* e *hardware*;

g) uma estrutura clara de notificação e formatos de relatórios acordados;

h) um processo claro e definido de gestão de mudanças;

i) política de controle de acesso, cobrindo:

1) as diferentes razões, requisitos e benefícios que justificam a necessidade do acesso pelo terceiro;

2) métodos de acesso permitido e o controle e uso de identificadores únicos, tais como identificadores de usuários e senhas de acesso;

3) um processo de autorização de acesso e privilégios para os usuários;

4) um requisito para manter uma lista de pessoas autorizadas a usar os serviços que estão sendo disponibilizados, e quais os seus direitos e privilégios com relação a tal uso;

5) uma declaração de que todo o acesso que não seja explicitamente autorizado é proibido;

6) um processo para revogar os direitos de acesso ou interromper a conexão entre sistemas;

j) dispositivos para relato, notificação e investigação de incidentes de segurança da informação e violação da segurança, bem como as violações dos requisitos definidos no acordo;

k) uma descrição do produto ou serviço que está sendo fornecido e uma descrição da informação que deve estar disponível, juntamente com a sua classificação de segurança (ver 7.2.1);

l) níveis de serviços acordados e os níveis de serviços inaceitáveis;

m) definição de critérios de desempenho verificáveis, seu monitoramento e relato;

n) direito de monitorar e revogar qualquer atividade relacionada com os ativos da organização;

o) direito de auditar as responsabilidades definidas do acordo, para ter essas auditorias realizadas por terceira parte para enumerar os direitos regulamentares dos auditores;

p) estabelecimento de um processo escalonado para resolução de problemas;

q) requisitos para a continuidade dos serviços, incluindo medições para disponibilidade e confiabilidade, de acordo com as prioridades do negócio da organização;

r) respectivas obrigações das partes com o acordo;

s) responsabilidades com relação a aspectos legais e como é assegurado que os requisitos legais são atendidos, por exemplo, leis de proteção de dados, levando-se em consideração especialmente os diferentes sistemas legais nacionais, se o acordo envolver a cooperação com organizações em outros países (ver 15.1);

t) direitos de propriedade intelectual e direitos autorais (ver 15.1.2) e proteção de qualquer trabalho colaborativo (ver 6.1.5);

u) envolvimento do terceiro com subfornecedores e os controles de segurança da informação que esses subfornecedores precisam implementar;

v) condições de renegociação ou encerramento de acordos:

   1) um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo;

   2) renegociação dos acordos se os requisitos de segurança da organização mudarem;

   3) listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos.

Informações adicionais
Os acordos podem variar consideravelmente para diferentes organizações e entre os diferentes tipos de terceiros. Portanto, convém que sejam tomados cuidados para incluir nos acordos todos os riscos identificados e os requisitos de segurança da informação (ver 6.2.1). Onde necessário, os procedimentos e controles requeridos podem ser incluídos em um plano de gestão de segurança da informação.

Se a gestão da segurança da informação for terceirizada, convém que os acordos definam como os terceiros irão garantir que a segurança da informação, conforme definida na análise/avaliação de riscos, será mantida e como a segurança da informação será adaptada para identificar e tratar com as mudanças aos riscos.

Algumas das diferenças entre as terceirizações e as outras formas de provisão de serviços de terceiros incluem a questão das obrigações legais, o planejamento do período de transição e de descontinuidade da operação durante este período, planejamento de contingências e análise crítica de investigações, e coleta e gestão de incidentes de segurança da informação. Portanto, é importante que a organização planeje e gerencie a transição para um terceirizado e tenha processos adequados implantados para gerenciar as mudanças e renegociar ou encerrar os acordos.

Os procedimentos para continuar processando no caso em que o terceiro se torne incapaz de prestar o serviço precisam ser considerados no acordo para evitar qualquer atraso nos serviços de substituição.

Acordos com terceiros podem também envolver outras partes. Convém que os acordos que concedam o acesso a terceiros incluam permissão para designação de outras partes elegíveis e condições para os seus acessos e envolvimento.

De um modo geral os acordos são geralmente elaborados pela organização. Podem existir situações onde, em algumas circunstâncias, um acordo possa ser elaborado e imposto à organização pelo terceiro. A organização precisa assegurar que a sua própria segurança da informação não é afetada desnecessariamente pelos requisitos do terceiro, estipulados no acordo imposto.

7 Gestão de ativos

7.1 Responsabilidade pelos ativos

Objetivo: Alcançar e manter a proteção adequada dos ativos da organização. Convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Convém que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanece responsável pela proteção adequada dos ativos.

7.1.1 Inventário dos ativos

Controle
Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.

Diretrizes para implementação
Convém que a organização identifique todos os ativos e documente a importância destes ativos. Convém que o inventário do ativo inclua todas as informações necessárias que permitam recuperar de um desastre, incluindo o tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças e a importância do ativo para o negócio. Convém que o inventário não duplique outros inventários desnecessariamente, porém ele deve assegurar que o seu conteúdo está coerente.

Adicionalmente, convém que o proprietário (ver 7.1.2) e a classificação da informação (ver 7.2) sejam acordados e documentados para cada um dos ativos. Convém que, com base na importância do ativo, seu valor para o negócio e a sua classificação de segurança, níveis de proteção proporcionais à importância dos ativos sejam identificados (mais informações sobre como valorar os ativos para indicar a sua importância podem ser encontradas na ISO IEC TR 13335-3).

Informações adicionais
Existem vários tipos de ativos, incluindo:

a) ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

b) ativos de *software*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

d) serviços: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;

e) pessoas e suas qualificações, habilidades e experiências;

f) intangíveis, tais como a reputação e a imagem da organização.

Os inventários de ativos ajudam a assegurar que a proteção efetiva do ativo pode ser feita e também pode ser requerido para outras finalidades do negócio, como saúde e segurança, seguro ou financeira (gestão de ativos). O processo de compilação de um inventário de ativos é um pré-requisito importante no gerenciamento de riscos (ver seção 4).

7.1.2 Proprietário dos ativos

Controle
Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário[2] designado por uma parte definida da organização.

Diretrizes para implementação
Convém que o proprietário do ativo seja responsável por:

a) assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificados;

b) definir e periodicamente analisar criticamente as classificações e restrições ao acesso, levando em conta as políticas de controle de acesso, aplicáveis.

O proprietário pode ser designado para:

a) um processo do negócio;

b) um conjunto de atividades definidas;

c) uma aplicação; ou

d) um conjunto de dados definido.

Informações adicionais
As tarefas de rotina podem ser delegadas, por exemplo, para um custodiante que cuida do ativo no dia-a-dia, porém a responsabilidade permanece com o proprietário.

Em sistemas de informação complexos pode ser útil definir grupos de ativos que atuem juntos para fornecer uma função particular, como serviços. Neste caso, o proprietário do serviço é o responsável pela entrega do serviço, incluindo o funcionamento dos ativos, que provê os serviços.

7.1.3 Uso aceitável dos ativos

Controle
Convém que sejam identificadas, documentadas e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.

Diretrizes para implementação
Convém que todos os funcionários, fornecedores e terceiros sigam as regras para o uso permitido de informações e de ativos associados aos recursos de processamento da informação, incluindo:

a) regras para o uso da internet e do correio eletrônico (ver 10.8);

b) diretrizes para o uso de dispositivos móveis, especialmente para o uso fora das instalações da organização (ver 11.7.1).

---

[2] O termo “proprietário” identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo.

Convém que regras específicas ou diretrizes sejam fornecidas pelo gestor relevante. Convém que funcionários, fornecedores e terceiros que usem ou tenham acesso aos ativos da organização estejam conscientes dos limites que existem para os usos das informações e ativos associados da organização aos recursos de processamento da informação. Convém que eles sejam responsáveis pelo uso de quaisquer recursos de processamento da informação e de quaisquer outros usos conduzidos sob a suas responsabilidades.

7.2 Classificação da informação

Objetivo: Assegurar que a informação receba um nível adequado de proteção.

Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

7.2.1 Recomendações para classificação

Controle
Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Diretrizes para implementação
Convém que a classificação da informação e seus respectivos controles de proteção levem em consideração as necessidades de compartilhamento ou restrição de informações e os respectivos impactos nos negócios, associados com tais necessidades.

Convém que as diretrizes para classificação incluam convenções para classificação inicial e reclassificação ao longo do tempo, de acordo com algumas políticas de controle de acesso predeterminadas (ver 11.1.1)

Convém que seja de responsabilidade do proprietário do ativo (ver 7.1.2) definir a classificação de um ativo, analisando-o criticamente a intervalos regulares, e assegurar que ele está atualizado e no nível apropriado. Convém que a classificação leve em consideração a agregação do efeito mencionado em 10.7.2.

Convém que cuidados sejam tomados com a quantidade de categorias de classificação e com os benefícios obtidos pelo seu uso. Esquemas excessivamente complexos podem tornar o uso incômodo e ser inviáveis economicamente ou impraticáveis. Convém que atenção especial seja dada na interpretação dos rótulos de classificação sobre documentos de outras organizações, que podem ter definições diferentes para rótulos iguais ou semelhantes aos usados.

Informações adicionais
O nível de proteção pode ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação, bem como quaisquer outros requisitos que sejam considerados.

A informação freqüentemente deixa de ser sensível ou crítica após um certo período de tempo, por exemplo quando a informação se torna pública. Convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de custos desnecessários, resultando em despesas adicionais.

Considerar, conjuntamente, documentos com requisitos de segurança similares, quando da atribuição dos níveis de classificação, pode ajudar a simplificar a tarefa de classificação.

Em geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida.

7.2.2 Rótulos e tratamento da informação

Controle

Convém que um conjunto apropriado de procedimentos para rotulação e tratamento da informação seja definido e implementado de acordo com o esquema de classificação adotado pela organização.

Diretrizes para implementação

Os procedimentos para rotulação da informação precisam abranger tanto os ativos de informação no formato físico quanto no eletrônico.

Convém que as saídas de sistemas que contêm informações classificadas como sensíveis ou críticas tenham o rótulo apropriado da classificação da informação (na saída). Convém que o rótulo reflita a classificação de acordo com as regras estabelecidas em 7.2.1. Itens que devem ser considerados incluem relatórios impressos, telas, mídias magnéticas (fitas, discos, CD), mensagens eletrônicas e transferências de arquivos.

Convém que sejam definidos, para cada nível de classificação, procedimentos para o tratamento da informação que contemplem o processamento seguro, a armazenagem, a transmissão, a reclassificação e a destruição. Convém que isto também inclua os procedimentos para a cadeia de custódia e registros de qualquer evento de segurança relevante.

Convém que acordos com outras organizações, que incluam o compartilhamento de informações, considerem procedimentos para identificar a classificação daquela informação e para interpretar os rótulos de classificação de outras organizacões.

Informações adicionais

A rotulação e o tratamento seguro da classificação da informação é um requisito-chave para os procedimentos de compartilhamento da informação. Os rótulos físicos são uma forma usual de rotulação. Entretanto, alguns ativos de informação, como documentos em forma eletrônica, não podem ser fisicamente rotulados, sendo necessário usar um rótulo eletrônico. Por exemplo, a notificação do rótulo pode aparecer na tela ou no *display*. Onde a aplicação do rótulo não for possível, outras formas de definir a classificação da informação podem ser usadas, por exemplo, por meio de procedimentos ou metadados.

8 Segurança em recursos humanos

8.1 Antes da contratação[3]

Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos.

Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis.

Convém que todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.

8.1.1 Papéis e responsabilidades

Controle
Convém que papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros sejam definidos e documentados de acordo com a política de segurança da informação da organização.

Diretrizes para implementação
Convém que os papéis e responsabilidades pela segurança da informação incluam requisitos para:

a) implementar e agir de acordo com as políticas de segurança da informação da organização (ver 5.1);

b) proteger ativos contra acesso não autorizado, divulgação, modificação, destruição ou interferência;

c) executar processos ou atividades particulares de segurança da informação;

d) assegurar que a responsabilidade é atribuída à pessoa para tomada de ações;

e) relatar eventos potenciais ou reais de segurança da informação ou outros riscos de segurança para a organização.

Convém que papéis e responsabilidades de segurança da informação sejam definidos e claramente comunicados aos candidatos a cargos, durante o processo de pré-contratação.

Informações adicionais
Descrições de cargos podem ser usadas para documentar responsabilidades e papéis pela segurança da informação. Convém que papéis e responsabilidades pela segurança da informação para pessoas que não estão engajadas por meio do processo de contratação da organização, como, por exemplo, através de uma organização terceirizada, sejam claramente definidos e comunicados.

[3] Explicação: A palavra “contratação”, neste contexto, visa cobrir todas as seguintes diferentes situações: contratação de pessoas (temporárias ou por longa duração), nomeação de funções, mudança de funções, atribuições de contratos e encerramento de quaisquer destas situações.

8.1.2 Seleção

Controle
Convém que verificações do histórico de todos os candidatos a emprego, fornecedores e terceiros sejam realizadas de acordo com a ética, as leis e as regulamentações pertinentes, e proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.

Diretrizes para implementação
Convém que as verificações levem em consideração toda a legislação pertinente relativa à privacidade, proteção de dados pessoais e/ou emprego, e onde permitido, incluam os seguintes itens:

a) disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal;

b) uma verificação (da exatidão e inteireza) das informações do *curriculum vitae* do candidato;

c) confirmação das qualificações acadêmicas e profissionais;

d) verificação independente da identidade (passaporte ou documento similar);

e) verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais.

Convém que a organização também faça verificações mais detalhadas, onde um trabalho envolver pessoas, tanto por contratação como por promoção, que tenham acesso aos recursos de processamento da informação, em particular aquelas que tratam de informações sensíveis, tais como informações financeiras ou informações altamente confidenciais.

Convém que os procedimentos definam critérios e limitações para as verificações de controle, por exemplo, quem está qualificado para selecionar as pessoas, e como, quando e por que as verificações de controle são realizadas.

Convém que um processo de seleção também seja feito para fornecedores e terceiros. Quando essas pessoas vêm por meio de uma agência, convém que o contrato especifique claramente as responsabilidades da agência pela seleção e os procedimentos de notificação que devem ser seguidos se a seleção não for devidamente concluída ou quando os resultados obtidos forem motivos de dúvidas ou preocupações. Do mesmo modo, convém que acordos com terceiros (ver 6.2.3) especifiquem claramente todas as responsabilidades e procedimentos de notificação para a seleção.

Convém que informações sobre todos os candidatos que estão sendo considerados para certas posições dentro da organização sejam levantadas e tratadas de acordo com qualquer legislação apropriada existente na jurisdição pertinente. Dependendo da legislação aplicável, convém que os candidatos sejam previamente informados sobre as atividades de seleção.

8.1.3 Termos e condições de contratação

Controle
Como parte das suas obrigações contratuais, convém que os funcionários, fornecedores e terceiros concordem e assinem os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e a da organização para a segurança da informação.

Diretrizes para implementação

Convém que os termos e condições de trabalho reflitam a política de segurança da organização, esclarecendo e declarando:

a) que todos os funcionários, fornecedores e terceiros que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação antes de lhes ser dado o acesso aos recursos de processamento da informação;

b) as responsabilidades legais e direitos dos funcionários, fornecedores e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais ou à legislação de proteção de dados (ver 15.1.1 e 15.1.2);

c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização associados com os sistemas de informação e com os serviços conduzidos pelos funcionários, fornecedores ou terceiros (ver 7.2.1 e 10.7.3);

d) as responsabilidades dos funcionários, fornecedores e terceiros pelo tratamento da informação recebida de outras companhias ou de partes externas;

e) responsabilidades da organização pelo tratamento das informações pessoais, incluindo informações pessoais criadas como resultado de, ou em decorrência da, contratação com a organização (ver 15.1.4);

f) responsabilidades que se estendem para fora das dependências da organização e fora dos horários normais de trabalho, como, por exemplo, nos casos de execução de trabalhos em casa (ver 9.2.5 e 11.7.1);

g) ações a serem tomadas no caso de o funcionário, fornecedor ou terceiro desrespeitar os requisitos de segurança da informação da organização (ver 8.2.3).

Convém que a organização assegure que os funcionários, fornecedores e terceiros concordam com os termos e condições relativas à segurança da informação adequados à natureza e extensão do acesso que eles terão aos ativos da organização associados com os sistemas e serviços de informação.

Convém que as responsabilidades contidas nos termos e condições de contratação continuem por um período de tempo definido, após o término da contratação (ver 8.3), onde apropriado.

Informações adicionais

Um código de conduta pode ser usado para contemplar as responsabilidades dos funcionários, fornecedores ou terceiros, em relação à confidencialidade, proteção de dados, éticas, uso apropriado dos recursos e dos equipamentos da organização, bem como práticas de boa conduta esperada pela organização. O fornecedor ou o terceiro pode estar associado com uma organização externa que possa, por sua vez, ser solicitada a participar de acordos contratuais, em nome do contratado.

8.2 Durante a contratação

Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.

Convém que as responsabilidades pela direção sejam definidas para garantir que a segurança da informação é aplicada em todo trabalho individual dentro da organização.

Convém que um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação seja fornecido para todos os funcionários, fornecedores e terceiros, para minimizar possíveis riscos de segurança da informação. Convém que um processo disciplinar formal para tratar das violações de segurança da informação seja estabelecido.

8.2.1 Responsabilidades da direção

Controle
Convém que a direção solicite aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

Diretrizes para implementação
Convém que as responsabilidades da direção assegurem que os funcionários, fornecedores e terceiros:

a) estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação antes de obter acesso às informações sensíveis ou aos sistemas de informação;

b) recebam diretrizes que definam quais as expectativas sobre a segurança da informação de suas atividades dentro da organização;

c) estão motivados para cumprir com as políticas de segurança da informação da organização;

d) atinjam um nível de conscientização sobre segurança da informação que seja relevante para os seus papéis e responsabilidades dentro da organização (ver 8.2.2);

e) atendam aos termos e condições de contratação, que incluam a política de segurança da informação da organização e métodos apropriados de trabalho;

f) tenham as habilidades e qualificações apropriadas.

Informações adicionais
Se os funcionários, fornecedores e terceiros não forem conscientizados das suas responsabilidades, eles podem causar consideráveis danos para a organização. Pessoas motivadas têm uma maior probabilidade de serem mais confiáveis e de causar menos incidentes de segurança da informação.

Uma má gestão pode causar às pessoas o sentimento de sub-valorização, resultando em um impacto de segurança da informação negativo para a organização. Por exemplo, uma má gestão pode levar a segurança da informação a ser negligenciada ou a um potencial mau uso dos ativos da organização.

8.2.2 Conscientização, educação e treinamento em segurança da informação

Controle
Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções.

Diretrizes para implementação
Convém que o treinamento em conscientização comece com um processo formal de indução concebido para introduzir as políticas e expectativas de segurança da informação da organização, antes que seja dado o acesso às informações ou serviços.

Convém que os treinamentos em curso incluam requisitos de segurança da informação, responsabilidades legais e controles do negócio, bem como o treinamento do uso correto dos recursos de processamento da informação, como, por exemplo, procedimentos de *log-on*, o uso de pacotes de *software* e informações sobre o processo disciplinar (ver 8.2.3).

Informações adicionais
Convém que a conscientização, educação e treinamento nas atividades de segurança da informação sejam adequados e relevantes para os papéis, responsabilidades e habilidades da pessoa, e que incluam informações sobre conhecimento de ameaças, quem deve ser contatado para orientações sobre segurança da informação e os canais adequados para relatar os incidentes de segurança da informação (ver 13.1).

O treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação, e respondam de acordo com as necessidades do seu trabalho.

8.2.3 Processo disciplinar

Controle
Convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.

Diretrizes para implementação
Convém que o processo disciplinar não inicie sem uma verificação prévia de que a violação da segurança da informação realmente ocorreu (ver 13.2.3 em coleta de evidências).

Convém que o processo disciplinar formal assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança da informação. O processo disciplinar formal deve dar uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores conforme requerido. Em casos sérios de má conduta, convém que o processo permita a imediata remoção das atribuições, direitos de acesso e privilégios e, dependendo da situação, solicitar à pessoa, a saída imediata das dependências da organização, escoltando-a.

Informações adicionais
Convém que o processo disciplinar também seja usado como uma forma de dissuasão, para evitar que os funcionários, fornecedores e terceiros violem os procedimentos e as políticas de segurança da informação da organização, e quaisquer outras violações na segurança.

8.3 Encerramento ou mudança da contratação

Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.

Convém que responsabilidades sejam definidas para assegurar que a saída de funcionários, fornecedores e terceiros da organização seja feita de modo controlado e que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso estão concluídas.

Convém que as mudanças de responsabilidades e de trabalhos dentro de uma organização sejam gerenciadas quando do encerramento da respectiva responsabilidade ou trabalho de acordo com esta seção, e quaisquer novos trabalhos sejam gerenciados conforme descrito em 8.1.

8.3.1 Encerramento de atividades

Controle
Convém que responsabilidades para realizar o encerramento ou a mudança de um trabalho sejam claramente definidas e atribuídas.

Diretrizes para implementação
Convém que a comunicação de encerramento de atividades inclua requisitos de segurança e responsabilidades legais existentes e, onde apropriado, responsabilidades contidas em quaisquer acordos de confidencialidade (ver 6.1.5) e os termos e condições de trabalho (ver 8.1.3) que continuem por um período definido após o fim do trabalho do funcionário, do fornecedor ou do terceiro.

Convém que as responsabilidades e obrigações contidas nos contratos dos funcionários, fornecedores ou terceiros permaneçam válidas após o encerramento das atividades.

Convém que as mudanças de responsabilidades ou do trabalho sejam gerenciadas quando do encerramento da respectiva responsabilidade ou do trabalho, e que novas responsabilidades ou trabalho sejam controladas conforme descrito em 8.1.

Informações adicionais
A função de Recursos Humanos é geralmente responsável pelo processo global de encerramento e trabalha em conjunto com o gestor responsável pela pessoa que está saindo, para gerenciar os aspectos de segurança da informação dos procedimentos pertinentes. No caso de um fornecedor, o processo de encerramento de atividades pode ser realizado por uma agência responsável pelo fornecedor e, no caso de um outro usuário, isto pode ser tratado pela sua organização.

Pode ser necessário informar aos funcionários, clientes, fornecedores ou terceiros sobre as mudanças de pessoal e procedimentos operacionais.

8.3.2 Devolução de ativos

Controle
Convém que todos os funcionários, fornecedores e terceiros devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

Diretrizes para implementação
Convém que o processo de encerramento de atividades seja formalizado para contemplar a devolução de todos os equipamentos, documentos corporativos e *software* entregues à pessoa. Outros ativos da organização, tais como dispositivos de computação móvel, cartões de créditos, cartões de acesso, *software*, manuais e informações armazenadas em mídia eletrônica, também precisam ser devolvidos.

No caso em que um funcionário, fornecedor ou terceiro compre o equipamento da organização ou use o seu próprio equipamento pessoal, convém que procedimentos sejam adotados para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento (ver 10.7.1).

Nos casos em que o funcionário, fornecedor ou terceiro tenha conhecimento de que seu trabalho é importante para as atividades que são executadas, convém que este conhecimento seja documentado e transferido para a organização.

8.3.3 Retirada de direitos de acesso

Controle
Convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.

Diretrizes para implementação
Convém que os direitos de acesso da pessoa aos ativos associados com os sistemas de informação e serviços sejam reconsiderados, após o encerramento das atividades. Isto irá determinar se é necessário retirar os direitos de acesso. Convém que mudanças de uma atividade sejam refletidas na retirada de todos os direitos de acesso que não foram aprovados para o novo trabalho. Convém que os direitos de acesso que sejam retirados ou adaptados incluam o acesso lógico e físico, chaves, cartões de identificação, recursos de processamento da informação (ver 11.2.4), subscrições e retirada de qualquer documentação que os identifiquem como um membro atual da organização. Caso o funcionário, fornecedor ou terceiro que esteja saindo tenha conhecimento de senhas de contas que permanecem ativas, convém que estas sejam alteradas após um encerramento das atividades, mudança do trabalho, contrato ou acordo.

Convém que os direitos de acesso aos ativos de informação e aos recursos de processamento da informação sejam reduzidos ou retirados antes que a atividade se encerre ou altere, dependendo da avaliação de fatores de risco, tais como:

a) se o encerramento da atividade ou a mudança é iniciada pelo funcionário, fornecedor ou terceiro, ou pelo gestor e a razão do encerramento da atividade;

b) as responsabilidades atuais do funcionário, fornecedor ou qualquer outro usuário;

c) valor dos ativos atualmente acessíveis.

Informações adicionais
Em certas circunstâncias os direitos de acesso podem ser alocados com base no que está sendo disponibilizado para mais pessoas do que as que estão saindo (funcionário, fornecedor ou terceiro), como, por exemplo, grupos de ID. Convém que, em tais casos, as pessoas que estão saindo da organização sejam retiradas de quaisquer listas de grupos de acesso e que sejam tomadas providências para avisar aos outros funcionários, fornecedores e terceiros envolvidos para não mais compartilhar estas informações com a pessoa que está saindo.

Nos casos em que o encerramento da atividade seja da iniciativa do gestor, os funcionários, fornecedores ou terceiros descontentes podem deliberadamente corromper a informação ou sabotar os recursos de processamento da informação. No caso de pessoas demitidas ou exoneradas, elas podem ser tentadas a coletar informações para uso futuro.

9 Segurança física e do ambiente

9.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

Convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados. Convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências.

Convém que a proteção oferecida seja compatível com os riscos identificados.

9.1.1 Perímetro de segurança física

Controle
Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação.

Diretrizes para a implementação
Convém que sejam levadas em consideração e implementadas as seguintes diretrizes para perímetros de segurança física, quando apropriado:

a) os perímetros de segurança sejam claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro, e dos resultados da análise/avaliação de riscos;

b) os perímetros de um edifício ou de um local que contenha instalações de processamento da informação sejam fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão); convém que as paredes externas do local sejam de construção robusta e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle, por exemplo, barras, alarmes, fechaduras etc.; convém que as portas e janelas sejam trancadas quando estiverem sem monitoração, e que uma proteção externa para as janelas seja considerada, principalmente para as que estiverem situadas no andar térreo;

c) seja implantada uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; o acesso aos locais ou edifícios deve ficar restrito somente ao pessoal autorizado;

d) sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;

e) todas as portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; elas devem funcionar de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas;

f) sistemas adequados de detecção de intrusos, de acordo com normas regionais, nacionais e internacionais, sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis; as áreas não ocupadas devem ser protegidas por alarmes o tempo todo; também deve ser dada proteção a outras áreas, por exemplo, salas de computadores ou salas de comunicações;

g) as instalações de processamento da informação gerenciadas pela organização devem ficar fisicamente separadas daquelas que são gerenciadas por terceiros.

Informações adicionais
Pode-se obter proteção física criando uma ou mais barreiras físicas ao redor das instalações e dos recursos de processamento da informação da organização. O uso de barreiras múltiplas proporciona uma proteção adicional, uma vez que neste caso a falha de uma das barreiras não significa que a segurança fique comprometida imediatamente.

Uma área segura pode ser um escritório trancável ou um conjunto de salas rodeado por uma barreira física interna contínua de segurança. Pode haver necessidade de barreiras e perímetros adicionais para o controle do acesso físico, quando existem áreas com requisitos de segurança diferentes dentro do perímetro de segurança.

Convém que sejam tomadas precauções especiais para a segurança do acesso físico no caso de edifícios que alojam diversas organizações.

9.1.2 Controles de entrada física

Controle
Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes:

a) a data e hora da entrada e saída de visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; convém que as permissões de acesso sejam concedidas somente para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência;

b) acesso às áreas em que são processadas ou armazenadas informações sensíveis seja controlado e restrito às pessoas autorizadas; convém que sejam utilizados controles de autenticação, por exemplo, cartão de controle de acesso mais PIN *(personal identification number)*, para autorizar e validar todos os acessos; deve ser mantido de forma segura um registro de todos os acessos para fins de auditoria;

c) seja exigido que todos os funcionários, fornecedores e terceiros, e todos os visitantes, tenham alguma forma visível de identificação, e eles devem avisar imediatamente o pessoal de segurança caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;

d) aos terceiros que realizam serviços de suporte, seja concedido acesso restrito às áreas seguras ou às instalações de processamento da informação sensível somente quando necessário; este acesso deve ser autorizado e monitorado;

e) os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário (ver 8.3.3).

9.1.3 Segurança em escritórios, salas e instalações

Controle
Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes para proteger escritórios, salas e instalações:

a) sejam levados em conta os regulamentos e normas de saúde e segurança aplicáveis;

b) as instalações-chave sejam localizadas de maneira a evitar o acesso do público;

c) os edifícios sejam discretos e dêem a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações, quando for aplicável;

d) as listas de funcionários e guias telefônicos internos que identifiquem a localização das instalações que processam informações sensíveis não fiquem facilmente acessíveis ao público.

9.1.4 Proteção contra ameaças externas e do meio ambiente

Controle
Convém que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

Diretrizes para implementação
Convém que sejam levadas em consideração todas as ameaças à segurança representadas por instalações vizinhas, por exemplo, um incêndio em um edifício vizinho, vazamento de água do telhado ou em pisos do subsolo ou uma explosão na rua.

Convém que sejam levadas em consideração as seguintes diretrizes para evitar danos causados por incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem:

a) os materiais perigosos ou combustíveis sejam armazenados a uma distância segura da área de segurança. Suprimentos em grande volume, como materiais de papelaria, não devem ser armazenados dentro de uma área segura;

b) os equipamentos para contingência e mídia de *backup* fiquem a uma distância segura, para que não sejam danificados por um desastre que afete o local principal;

c) os equipamentos apropriados de detecção e combate a incêndios sejam providenciados e posicionados corretamente.

9.1.5 Trabalhando em áreas seguras

Controle
Convém que seja projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes:

a) pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário;

b) seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas;

c) as áreas seguras não ocupadas sejam fisicamente trancadas e periodicamente verificadas;

d) não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

As normas para o trabalho em áreas seguras incluem o controle dos funcionários, fornecedores e terceiros que trabalham em tais áreas, bem como o controle de outras atividades de terceiros nestas áreas.

9.1.6 Acesso do público, áreas de entrega e de carregamento

Controle
Convém que os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes:

a) acesso a uma área de entrega e carregamento a partir do exterior do prédio fique restrito ao pessoal identificado e autorizado;

b) as áreas de entrega e carregamento sejam projetadas de tal maneira que seja possível descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

c) as portas externas de uma área de entrega e carregamento sejam protegidas enquanto as portas internas estiverem abertas;

d) os materiais entregues sejam inspecionados para detectar ameaças potenciais (ver 9.2.1d)) antes de serem transportados da área de entrega e carregamento para o local de utilização;

e) os materiais entregues sejam registrados por ocasião de sua entrada no local, usando-se procedimentos de gerenciamento de ativos (ver 7.1.1);

f) as remessas entregues sejam segregadas fisicamente das remessas que saem, sempre que possível.

9.2 Segurança de equipamentos

Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização.

Convém que os equipamentos sejam protegidos contra ameaças físicas e do meio ambiente.

A proteção dos equipamentos (incluindo aqueles utilizados fora do local, e a retirada de ativos) é necessária para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos. Convém que também seja levado em consideração a introdução de equipamentos no local, bem como sua remoção. Podem ser necessários controles especiais para a proteção contra ameaças físicas e para a proteção de instalações de suporte, como a infra-estrutura de suprimento de energia e de cabeamento.

9.2.1 Instalação e proteção do equipamento

Controle
Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes para proteger os equipamentos:

a) os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;

b) as instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas de forma que o ângulo de visão seja restrito, de modo a reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização, e os locais de armazenagem sejam protegidos, a fim de evitar o acesso não autorizado;

c) os itens que exigem proteção especial devem ser isolados para reduzir o nível geral de proteção necessário;

d) sejam adotados controles para minimizar o risco de ameaças físicas potenciais, tais como furto ou roubo, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

e) sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;

f) as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente os recursos de processamento da informação;

g) todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

h) para equipamentos em ambientes industriais, o uso de métodos especiais de proteção, tais como membranas para teclados, deve ser considerado;

i) os equipamentos que processam informações sensíveis sejam protegidos, a fim de minimizar o risco de vazamento de informações em decorrência de emanações.

9.2.2 Utilidades

Controle
Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Diretrizes para implementação
Convém que todas as utilidades, tais como suprimento de energia elétrica, suprimento de água, esgotos, calefação/ventilação e ar-condicionado sejam adequados para os sistemas que eles suportam. Convém que as utilidades sejam inspecionadas em intervalos regulares e testadas de maneira apropriada para assegurar seu funcionamento correto e reduzir os riscos de defeitos ou interrupções do funcionamento. Convém que seja providenciado um suprimento adequado de energia elétrica, de acordo com as especificações do fabricante dos equipamentos.

Recomenda-se o uso de UPS para suportar as paradas e desligamento dos equipamentos ou para manter o funcionamento contínuo dos equipamentos que suportam operações críticas dos negócios. Convém que hajam planos de contingência de energia referentes às providências a serem tomadas em caso de falha do UPS. Convém que seja considerado um gerador de emergência caso seja necessário que o processamento continue mesmo se houver uma interrupção prolongada do suprimento de energia. Convém que esteja disponível um suprimento adequado de combustível para garantir a operação prolongada do gerador. Convém que os equipamentos UPS e os geradores sejam verificados em intervalos regulares para assegurar que eles tenham capacidade adequada, e sejam testados de acordo com as recomendações do fabricante. Além disto, deve ser considerado o uso de múltiplas fontes de energia ou de uma subestação de força separada, se o local for grande.

Convém que as chaves de emergência para o desligamento da energia fiquem localizadas na proximidade das saídas de emergência das salas de equipamentos, para facilitar o desligamento rápido da energia em caso de uma emergência. Convém que seja providenciada iluminação de emergência para o caso de queda da força.

Convém que o suprimento de água seja estável e adequado para abastecer os equipamentos de ar-condicionado e de umidificação, bem como os sistemas de extinção de incêndios (quando usados). Falhas de funcionamento do abastecimento de água podem danificar o sistema ou impedir uma ação eficaz de extinção de incêndios. Convém que seja analisada a necessidade de sistemas de alarme para detectar falhas de funcionamento das utilidades, instalando os alarmes, se necessário.

Convém que os equipamentos de telecomunicações sejam conectados à rede pública de energia elétrica através de pelo menos duas linhas separadas, para evitar que a falha de uma das conexões interrompa os serviços de voz. Convém que os serviços de voz sejam adequados para atender às exigências legais locais relativas a comunicações de emergência.

Informações adicionais
As opções para assegurar a continuidade do suprimento de energia incluem múltiplas linhas de entrada, para evitar que uma falha em um único ponto comprometa o suprimento de energia.

9.2.3 Segurança do cabeamento

Controle
Convém que o cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações seja protegido contra interceptação ou danos.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento:

a) as linhas de energia e de telecomunicações que entram nas instalações de processamento da informação sejam subterrâneas (ou fiquem abaixo do piso), sempre que possível, ou recebam uma proteção alternativa adequada;

b) cabeamento de redes seja protegido contra interceptação não autorizada ou danos, por exemplo, pelo uso de conduítes ou evitando trajetos que passem por áreas públicas;

c) os cabos de energia sejam segregados dos cabos de comunicações, para evitar interferências;

d) nos cabos e nos equipamentos, sejam utilizadas marcações claramente identificáveis, a fim de minimizar erros de manuseio, como, por exemplo, fazer de forma acidental conexões erradas em cabos da rede;

e) seja utilizada uma lista de documentação das conexões para reduzir a possibilidade de erros;

f) para sistemas sensíveis ou críticos, os seguintes controles adicionais devem ser considerados:

   1) instalação de conduítes blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais;

   2) uso de rotas alternativas e/ou meios de transmissão alternativos que proporcionem segurança adequada;

   3) utilização de cabeamento de fibras ópticas;

   4) utilização de blindagem eletromagnética para a proteção dos cabos;

   5) realização de varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos;

   6) acesso controlado aos painéis de conexões e às salas de cabos.

9.2.4 Manutenção dos equipamentos

Controle
Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanentes.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes para a manutenção dos equipamentos:

a) a manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor, e de acordo com as suas especificações;

b) a manutenção e os consertos dos equipamentos sejam realizados somente por pessoal de manutenção autorizado;

c) sejam mantidos os registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;

d) sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo de a manutenção ser realizada pelo pessoal do local ou por pessoal externo à organização; onde necessário, as informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança;

e) sejam atendidas todas as exigências estabelecidas nas apólices de seguro.

9.2.5 Segurança de equipamentos fora das dependências da organização

Controle
Convém que sejam tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

Diretrizes para implementação
Convém que, independentemente de quem seja o proprietário, a utilização de quaisquer equipamentos de processamento de informações fora das dependências da organização seja autorizada pela gerência.

Convém que sejam levadas em consideração as seguintes diretrizes para a proteção de equipamentos usados fora das dependências da organização:

a) os equipamentos e mídias removidos das dependências da organização não fiquem sem supervisão em lugares públicos; os computadores portáteis sejam carregados como bagagem de mão e disfarçados, sempre que possível, quando se viaja;

b) sejam observadas a qualquer tempo as instruções do fabricante para a proteção do equipamento, por exemplo, proteção contra a exposição a campos eletromagnéticos intensos;

c) os controles para o trabalho em casa sejam determinados por uma análise/avaliação de riscos, sendo aplicados controles adequados para cada caso, por exemplo, arquivos trancáveis, política de "mesa limpa", controles de acesso a computadores, e comunicação segura com o escritório (ver ISO/IEC 18028 – *Network security*);

d) haja uma cobertura adequada de seguro para proteger os equipamentos fora das dependências da organização.

Os riscos de segurança, por exemplo, de danos, furto ou espionagem, podem variar consideravelmente de um local para outro e convém que sejam levados em conta para determinar os controles mais apropriados.

Informações adicionais
Os equipamentos de armazenagem e processamento de informações incluem todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, cartões inteligentes, papéis e outros tipos, utilizados no trabalho em casa, ou que são removidos do local normal de trabalho.

Mais informações sobre outros aspectos da proteção de equipamentos móveis podem ser encontradas em 11.7.1.

9.2.6 Reutilização e alienação segura de equipamentos

Controle
Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.

Diretrizes para implementação
Convém que os dispositivos que contenham informações sensíveis sejam destruídos fisicamente ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.

Informações adicionais
No caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessária uma análise/avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo.

As informações podem ser comprometidas por um descarte feito sem os devidos cuidados ou pela reutilização do equipamento (ver 10.7.2).

9.2.7 Remoção de propriedade

Controle
Convém que equipamentos, informações ou *software* não sejam retirados do local sem autorização prévia.

Diretrizes para implementação
Convém que sejam levadas em consideração as seguintes diretrizes:

a) os equipamentos, informações ou *software* não sejam retirados do local sem autorização prévia;

b) os funcionários, fornecedores e terceiros que tenham autoridade para permitir a remoção de ativos para fora do local sejam claramente identificados;

c) sejam estabelecidos limites de tempo para a retirada de equipamentos do local, e a devolução seja controlada;

d) sempre que necessário ou apropriado, seja feito um registro da retirada e da devolução de equipamentos, quando do seu retorno.

Informações adicionais
Podem ser feitas inspeções aleatórias para detectar a retirada não autorizada de bens e a existência de equipamentos de gravação não autorizados, armas etc., e impedir sua entrada no local. Convém que tais inspeções aleatórias sejam feitas de acordo com a legislação e as normas aplicáveis. Convém que as pessoas sejam avisadas da realização das inspeções, e elas só podem ser feitas com a devida autorização, levando em conta as exigências legais e regulamentares.

10 Gerenciamento das operações e comunicações

10.1 Procedimentos e responsabilidades operacionais

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

Convém que os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos. Isto abrange o desenvolvimento de procedimentos operacionais apropriados.

Convém que seja utilizada a segregação de funções quando apropriado, para reduzir o risco de mau uso ou uso doloso dos sistemas.

10.1.1 Documentação dos procedimentos de operação

Controle
Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

Diretrizes para implementação
Convém que procedimentos documentados sejam preparados para as atividades de sistemas associadas a recursos de processamento e comunicação de informações, tais como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança (*backup*), manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

Convém que os procedimentos de operação especifiquem as instruções para a execução detalhada de cada tarefa, incluindo:

a) processamento e tratamento da informação;

b) *backup* (ver 10.5);

c) requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa;

d) instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema (ver 11.5.4);

e) dados para contatos de suporte para o caso de eventos operacionais inesperados ou dificuldades técnicas;

f) instruções especiais quanto ao manuseio e saída de mídias, tais como o uso de formulários especiais ou o gerenciamento de saídas confidenciais, incluindo procedimentos para o descarte seguro de resultados provenientes de rotinas com falhas (ver 10.7.2 e 10.7.3);

g) procedimento para o reinício e recuperação em caso de falha do sistema;

h) gerenciamento de trilhas de auditoria e informações de registros (*log*) de sistemas (ver 10.10).

Convém que procedimentos operacionais e os procedimentos documentados para atividades de sistemas sejam tratados como documentos formais e as mudanças sejam autorizadas pela direção. Quando tecnicamente possível, convém que os sistemas de informação sejam gerenciados uniformemente, usando os mesmos procedimentos, ferramentas e utilitários.

10.1.2 Gestão de mudanças

Controle
Convém que modificações nos recursos de processamento da informação e sistemas sejam controladas.

Diretrizes para implementação
Convém que sistemas operacionais e aplicativos estejam sujeitos a rígido controle de gestão de mudanças. Em particular, convém que os seguintes itens sejam considerados:

a) identificação e registro das mudanças significativas;

b) planejamento e testes das mudanças;

c) avaliação de impactos potenciais, incluindo impactos de segurança, de tais mudanças;

d) procedimento formal de aprovação das mudanças propostas;

e) comunicação dos detalhes das mudanças para todas as pessoas envolvidas;

f) procedimentos de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

Convém que sejam estabelecidos os procedimentos e responsabilidades gerenciais formais para garantir que haja um controle satisfatório de todas as mudanças em equipamentos, *software* ou procedimentos. Quando mudanças forem realizadas, convém que seja mantido um registro de auditoria contendo todas as informações relevantes.

Informações adicionais
O controle inadequado de modificações nos sistemas e nos recursos de processamento da informação é uma causa comum de falhas de segurança ou de sistema. Mudanças a ambientes operacionais, especialmente quando da transferência de um sistema em desenvolvimento para o estágio operacional, podem trazer impactos à confiabilidade de aplicações (ver 12.5.1).

Convém que mudanças em sistemas operacionais sejam apenas realizadas quando houver uma razão de negócio válida para tal, como um aumento no risco do sistema. A atualização de sistemas às versões mais atuais de sistemas operacionais ou aplicativos nem sempre é do interesse do negócio, pois pode introduzir mais vulnerabilidades e instabilidades ao ambiente do que a versão corrente. Pode haver ainda a necessidade de treinamento adicional, custos de licenciamento, suporte, manutenção e sobrecarga de administração, bem como a necessidade de novos equipamentos, especialmente durante a fase de migração.

10.1.3 Segregação de funções

Controle
Convém que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

Diretrizes para implementação
A segregação de funções é um método para redução do risco de uso indevido acidental ou deliberado dos sistemas. Convém que sejam tomados certos cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção. Convém que o início de um evento seja separado de sua autorização. Convém que a possibilidade de existência de conluios seja considerada no projeto dos controles.

As pequenas organizações podem considerar a segregação de funções difícil de ser implantada, mas convém que o seu princípio seja aplicado sempre que possível e praticável. Onde for difícil a segregação, convém que outros controles, como a monitoração das atividades, trilhas de auditoria e o acompanhamento gerencial, sejam considerados. É importante que a auditoria da segurança permaneça como uma atividade independente.

10.1.4 Separação dos recursos de desenvolvimento, teste e de produção

Controle
Convém que recursos de desenvolvimento, teste e produção sejam separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

Diretrizes para implementação
Convém que o nível de separação dos ambientes de produção, testes e desenvolvimento que é necessário para prevenir problemas operacionais seja identificado e os controles apropriados sejam implementados.

Convém que os seguintes itens sejam considerados:

a) as regras para a transferência de *software* da situação de desenvolvimento para a de produção sejam definidas e documentadas;

b) *software* em desenvolvimento e o *software* em produção sejam, sempre que possível, executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios;

c) os compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas não sejam acessíveis a partir de sistemas operacionais, quando não for necessário;

d) os ambientes de testes emulem o ambiente de produção o mais próximo possível;

e) os usuários tenham diferentes perfis para sistemas em testes e em produção, e que os menus mostrem mensagens apropriadas de identificação para reduzir o risco de erro;

f) os dados sensíveis não sejam copiados para os ambientes de testes (ver 12.4.2).

Informações adicionais
As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações inesperadas em arquivos ou sistemas ou falhas de sistemas. Nesse caso, é necessária a manutenção de um ambiente conhecido e estável, no qual possam ser executados testes significativos e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento.

Quando o pessoal de desenvolvimento e teste possui acesso ao ambiente de produção e suas informações, eles podem introduzir códigos não testados e não autorizados, ou mesmo alterar os dados do sistema. Em alguns sistemas essa capacidade pode ser mal utilizada para a execução de fraudes, ou introdução de códigos maliciosos ou não testados, que podem causar sérios problemas operacionais.

O pessoal de desenvolvimento e testes também representa uma ameaça à confidencialidade das informações de produção. As atividades de desenvolvimento e teste podem causar modificações não intencionais no *software* e informações se eles compartilharem o mesmo ambiente computacional. A separação dos ambientes de desenvolvimento, teste e produção são, portanto, desejável para reduzir o risco de modificações acidentais ou acessos não autorizados aos sistemas operacionais e aos dados do negócio (ver 12.4.2 para a proteção de dados de teste).

10.2 Gerenciamento de serviços terceirizados

Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

Convém que a organização verifique a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros.

10.2.1 Entrega de serviços

Controle
Convém que seja garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.

Diretrizes para implementação
Convém que a entrega de serviços por um terceiro inclua os arranjos de segurança acordados, definições de serviço e aspectos de gerenciamento de serviços. No caso de acordos de terceirização, convém que a organização planeje as transições necessárias (de informação, recursos de processamento de informações e quaisquer outros que necessitem de movimentação) e garanta que a segurança seja mantida durante todo o período de transição.

Convém que a organização garanta que o terceiro mantenha capacidade de serviço suficiente, juntamente com planos viáveis projetados para garantir que os níveis de continuidade de serviços acordados sejam mantidos após falhas de serviços severas ou desastres (ver 14.1).

10.2.2 Monitoramento e análise crítica de serviços terceirizados

Controle
Convém que os serviços, relatórios e registros fornecidos por terceiro sejam regularmente monitorados e analisados criticamente, e que auditorias sejam executadas regularmente.

Diretrizes para implementação
Convém que a monitoração e análise crítica dos serviços terceirizados garantam a aderência entre os termos de segurança de informação e as condições dos acordos, e que problemas e incidentes de segurança da informação sejam gerenciados adequadamente. Convém que isto envolva processos e relações de gerenciamento de serviço entre a organização e o terceiro para:

a) monitorar níveis de desempenho de serviço para verificar aderência aos acordos;

b) analisar criticamente os relatórios de serviços produzidos por terceiros e agendamento de reuniões de progresso conforme requerido pelos acordos;

c) fornecer informações acerca de incidentes de segurança da informação e análise crítica de tais informações tanto pelo terceiro quanto pela organização, como requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apóiem;

d) analisar criticamente as trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;

e) resolver e gerenciar quaisquer problemas identificados.

Convém que a responsabilidade do gerenciamento de relacionamento com o terceiro seja atribuída a um indivíduo designado ou equipe de gerenciamento de serviço. Adicionalmente, convém que a organização garanta que o terceiro atribua responsabilidades pela verificação de conformidade e reforço aos requisitos dos acordos. Convém que habilidades técnicas suficientes e recursos sejam disponibilizados para monitorar se os requisitos dos acordos (ver 6.2.3), em particular os requisitos de segurança da informação, estão sendo atendidos. Convém que ações apropriadas sejam tomadas quando deficiências na entrega dos serviços forem observadas.

Convém que a organização mantenha suficiente controle geral e visibilidade em todos os aspectos de segurança para as informações sensíveis ou críticas ou para os recursos de processamento da informação acessados, processados ou gerenciados por um terceiro. Convém que a organização garanta a retenção da visibilidade nas atividades de segurança como gerenciamento de mudanças, identificação de vulnerabilidades e relatório/resposta de incidentes de segurança da informação através de um processo de notificação, formatação e estruturação claramente definido.

Informações adicionais
Em caso de terceirização, a organização precisa estar ciente de que a responsabilidade final pela informação processada por um parceiro de terceirização permanece com a organização.

10.2.3 Gerenciamento de mudanças para serviços terceirizados

Controle
Convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.

Diretrizes para implementação
O processo de gerenciamento de mudanças para serviços terceirizados precisa levar em conta:

a) mudanças feitas pela organização para a implementação de:

   1) melhorias dos serviços correntemente oferecidos;

   2) desenvolvimento de quaisquer novas aplicações ou sistemas;

   3) modificações ou atualizações das políticas e procedimentos da organização;

   4) novos controles para resolver os incidentes de segurança da informação e para melhorar a segurança;

b) mudanças em serviços de terceiros para implementação de:

   1) mudanças e melhorias em redes;

   2) uso de novas tecnologias;

   3) adoção de novos produtos ou novas versões;

   4) novas ferramentas e ambientes de desenvolvimento;

   5) mudanças de localização física dos recursos de serviços;

   6) mudanças de fornecedores.

10.3 Planejamento e aceitação dos sistemas

Objetivo: Minimizar o risco de falhas nos sistemas.

O planejamento e a preparação prévios são requeridos para garantir a disponibilidade adequada de capacidade e recursos para entrega do desempenho desejado ao sistema.

Convém que projeções de requisitos de capacidade futura sejam feitas para reduzir o risco de sobrecarga dos sistemas.

Convém que os requisitos operacionais dos novos sistemas sejam estabelecidos, documentados e testados antes da sua aceitação e uso.

10.3.1 Gestão de capacidade

Controle
Convém que a utilização dos recursos seja monitorada e ajustada, e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.

Diretrizes para implementação
Convém que requisitos de capacidade sejam identificados para cada atividade nova ou em andamento. Convém que o ajuste e o monitoramento dos sistemas sejam aplicados para garantir e, quando necessário, melhorar a disponibilidade e eficiência dos sistemas. Convém que controles detectivos sejam implantados para identificar problemas em tempo hábil. Convém que projeções de capacidade futura levem em consideração os requisitos de novos negócios e sistemas e as tendências atuais e projetadas de capacidade de processamento de informação da organização.

Atenção particular precisa ser dada a qualquer recurso que possua um ciclo de renovação ou custo maior, sendo responsabilidade dos gestores monitorar a utilização dos recursos-chave dos sistemas. Convém que eles identifiquem as tendências de utilização, particularmente em relação às aplicações do negócio ou às ferramentas de gestão de sistemas de informação.

Convém que os gestores utilizem essas informações para identificar e evitar os potenciais gargalos e a dependência em pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços, e planejar ação corretiva apropriada.

10.3.2 Aceitação de sistemas

Controle
Convém que sejam estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.

Diretrizes para implementação
Convém que os gestores garantam que os requisitos e critérios para aceitação de novos sistemas estejam claramente definidos, acordados, documentados e testados. Convém que novos sistemas de informação, atualizações e novas versões só sejam migrados para produção após a obtenção de aceitação formal. Convém que os seguintes itens sejam considerados antes que a aceitação formal seja emitida:

a) requisitos de desempenho e de capacidade computacional;

b) recuperação de erros, procedimentos de reinicialização e planos de contingência;

c) preparação e teste de procedimentos operacionais de rotina, com base em normas definidas;

d) concordância sobre o conjunto de controles de segurança utilizados;

e) procedimentos manuais eficazes;

f) requisitos de continuidade dos negócios (ver 14.1);

g) evidência de que a instalação do novo sistema não afetará de forma adversa os sistemas existentes, particularmente nos períodos de pico de processamento, como, por exemplo, em final de mês;

h) evidência de que tenha sido considerado o impacto do novo sistema na segurança da organização como um todo;

i) treinamento na operação ou uso de novos sistemas;

j) facilidade de uso, uma vez que afeta o desempenho do usuário e evita falhas humanas.

Para os principais novos desenvolvimentos, convém que os usuários e as funções de operação sejam consultados em todos os estágios do processo de desenvolvimento, de forma a garantir a eficiência operacional do projeto de sistema proposto. Convém que os devidos testes sejam executados para garantir que todos os critérios de aceitação tenham sido plenamente satisfeitos.

Informações adicionais
A aceitação pode incluir um processo formal de certificação e reconhecimento para garantir que os requisitos de segurança tenham sido devidamente endereçados.

10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

Os recursos de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como vírus de computador, *worms* de rede, cavalos de Tróia e bombas lógicas. Convém que os usuários estejam conscientes dos perigos do código malicioso. Convém que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis.

10.4.1 Controles contra códigos maliciosos

Controle
Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Diretrizes para implementação
Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Convém que as seguintes diretrizes sejam consideradas:

a) estabelecer uma política formal proibindo o uso de *softwares* não autorizados (ver 15.1.2);

b) estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas;

c) conduzir análises críticas regulares dos *softwares* e dados dos sistemas que suportam processos críticos de negócio; convém que a presença de quaisquer arquivos não aprovados ou atualização não autorizada seja formalmente investigada;

d) instalar e atualizar regularmente *softwares* de detecção e remoção de códigos maliciosos para o exame de computadores e mídias magnéticas, de forma preventiva ou de forma rotineira; convém que as verificações realizadas incluam:

   1) verificação, antes do uso, da existência de códigos maliciosos nos arquivos em mídias óticas ou eletrônicas, bem como nos arquivos transmitidos através de redes;

   2) verificação, antes do uso, da existência de *software* malicioso em qualquer arquivo recebido através de correio eletrônico ou importado (*download*). Convém que essa avaliação seja feita em diversos locais, como, por exemplo, nos servidores de correio eletrônico, nos computadores pessoais ou quando da sua entrada na rede da organização;

   3) verificação da existência de códigos maliciosos em páginas *web*;

e) definir procedimentos de gerenciamento e respectivas responsabilidades para tratar da proteção de código malicioso nos sistemas, treinamento nesses procedimentos, reporte e recuperação de ataques de códigos maliciosos (ver 13.1 e 13.2);

f) preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos, incluindo todos os procedimentos necessários para a cópia e recuperação dos dados e *softwares* (ver seção 14);

g) implementar procedimentos para regularmente coletar informações, tais como, assinaturas de listas de discussão e visitas a *sites* informativos sobre novos códigos maliciosos;

h) implementar procedimentos para a verificação de informação relacionada a códigos maliciosos e garantia de que os boletins com alertas sejam precisos e informativos; convém que os gestores garantam que fontes qualificadas, como, por exemplo, jornais com reputação idônea, *sites* confiáveis ou fornecedores de *software* de proteção contra códigos maliciosos, sejam utilizadas para diferenciar boatos de notícias reais sobre códigos maliciosos; convém que todos os usuários estejam cientes dos problemas decorrentes de boatos e capacitados a lidar com eles.

Informações adicionais
A utilização de dois ou mais tipos de *software* de controle contra códigos maliciosos de diferentes fornecedores no ambiente de processamento da informação pode aumentar a eficácia na proteção contra códigos maliciosos.

Softwares de proteção contra código malicioso podem ser instalados para prover atualizações automáticas dos arquivos de definição e mecanismos de varredura, para garantir que a proteção esteja atualizada. Adicionalmente, estes *softwares* podem ser instalados em todas as estações de trabalho para a realização de verificações automáticas.

Convém que seja tomado cuidado quanto a possível introdução de códigos maliciosos durante manutenções e quando estão sendo realizados procedimentos de emergência. Tais procedimentos podem ignorar controles normais de proteção contra códigos maliciosos.

10.4.2 Controles contra códigos móveis

Controle
Onde o uso de códigos móveis é autorizado, convém que a configuração garanta que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e códigos móveis não autorizados tenham sua execução impedida.

Diretrizes para implementação
Convém que as seguintes ações sejam consideradas para proteger contra ações não autorizadas realizadas por códigos móveis:

a) executar códigos móveis em ambientes isolados logicamente;

b) bloquear qualquer tipo de uso de código móvel;

c) bloquear o recebimento de códigos móveis;

d) ativar medidas técnicas disponíveis nos sistemas específicos para garantir que o código móvel esteja sendo administrado;

e) controlar os recursos disponíveis para acesso ao código móvel;

f) estabelecer controles criptográficos de autenticação exclusiva do código móvel.

Informações adicionais
Código móvel é um código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário. Códigos móveis são associados a uma variedade de serviços *middleware*.

Além de garantir que os códigos móveis não carreguem códigos maliciosos, manter o controle deles é essencial na prevenção contra o uso não autorizado ou interrupção de sistemas, redes ou aplicativos, e na prevenção contra violações de segurança da informação.

10.5 Cópias de segurança

Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

Convém que procedimentos de rotina sejam estabelecidos para implementar as políticas e estratégias definidas para a geração de cópias de segurança (ver 14.1) e possibilitar a geração das cópias de segurança dos dados e sua recuperação em um tempo aceitável.

10.5.1 Cópias de segurança das informações

Controle
Convém que as cópias de segurança das informações e dos *softwares* sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

Diretrizes para implementação
Convém que recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e *software* essenciais possam ser recuperados após um desastre ou a falha de uma mídia.

Convém que os seguintes itens para a geração das cópias de segurança sejam considerados:

a) definição do nível necessário das cópias de segurança das informações;

b) produção de registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação;

c) a extensão (por exemplo, completa ou diferencial) e a freqüência da geração das cópias de segurança reflita os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;

d) as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

e) deve ser dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver seção 9), consistente com as normas aplicadas na instalação principal; os controles aplicados às mídias na instalação principal sejam usados no local das cópias de segurança;

f) as mídias de cópias de segurança sejam testadas regularmente para garantir que elas são suficientemente confiáveis para uso de emergência, quando necessário;

g) os procedimentos de recuperação sejam verificados e testados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação;

h) em situações onde a confidencialidade é importante, cópias de segurança sejam protegidas através de encriptação.

Convém que as cópias de segurança de sistemas específicos sejam testadas regularmente para garantir que elas estão aderentes aos requisitos definidos nos planos de continuidade do negócio (ver seção 14). Para sistemas críticos, convém que os mecanismos de geração de cópias de segurança abranjam todos os sistemas de informação, aplicações e dados necessários para a completa recuperação do sistema em um evento de desastre.

Convém que o período de retenção para informações essenciais ao negócio e também qualquer requisito para que cópias de arquivo sejam permanentemente retidas seja determinado (ver 15.1.3).

Informações adicionais
Os mecanismos de cópias de segurança podem ser automatizados para facilitar os processos de geração e recuperação das cópias de segurança. Convém que tais soluções automatizadas sejam suficientemente testadas antes da implementação e verificadas em intervalos regulares.

10.6 Gerenciamento da segurança em redes

Objetivo: Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.

O gerenciamento seguro de redes, que pode ir além dos limites da organização, requer cuidadosas considerações relacionadas ao fluxo de dados, implicações legais, monitoramento e proteção.

Controles adicionais podem ser necessários para proteger informações sensíveis trafegando sobre redes públicas.

10.6.1 Controles de redes

Controle
Convém que as redes sejam adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.

Diretrizes para implementação
Convém que gestores de redes implementem controles para garantir a segurança da informação nestas redes e a proteção dos serviços a elas conectadas, de acesso não autorizado. Em particular, convém que os seguintes itens sejam considerados:

a) a responsabilidade operacional pelas redes seja separada da operação dos recursos computacionais onde for apropriado (ver 10.1.3);

b) as responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos, incluindo equipamentos em áreas de usuários, sejam estabelecidos;

c) os controles especiais sejam estabelecidos para proteção da confidencialidade e integridade dos dados trafegando sobre redes públicas ou sobre as redes sem fio (*wireless*) e para proteger os sistemas e aplicações a elas conectadas (ver 11.4 e 12.3); controles especiais podem também ser requeridos para manter a disponibilidade dos serviços de rede e computadores conectados;

d) os mecanismos apropriados de registro e monitoração sejam aplicados para habilitar a gravação das ações relevantes de segurança;

e) as atividades de gerenciamento sejam coordenadas para otimizar os serviços para a organização e assegurar que os controles estejam aplicados de forma consistente sobre toda a infra-estrutura de processamento da informação.

Informações adicionais
Informações adicionais sobre segurança de redes podem ser encontradas na ISO/IEC 18028, *Information technology – Security techniques – IT network security*.

10.6.2 Segurança dos serviços de rede

Controle
Convém que as características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente ou terceirizados.

Diretrizes para implementação
Convém que a capacidade do provedor dos serviços de rede de gerenciar os serviços acordados de maneira segura seja determinada e monitorada regularmente, bem como que o direito de auditá-los seja acordado.

Convém que as definições de segurança necessárias para serviços específicos, como características de segurança, níveis de serviço e requisitos de gerenciamento, sejam identificadas. Convém que a organização assegure que os provedores dos serviços de rede implementam estas medidas.

Informações adicionais
Serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como *firewalls* e sistemas de detecção de intrusos. Estes serviços podem abranger desde o simples fornecimento de banda de rede não gerenciada até complexas ofertas de soluções de valor agregado.

Funcionalidades de segurança de serviços de rede podem ser:

a) tecnologias aplicadas para segurança de serviços de redes como autenticação, encriptação e controles de conexões de rede;

b) parâmetro técnico requerido para uma conexão segura com os serviços de rede de acordo com a segurança e regras de conexão de redes;

c) procedimentos para o uso de serviços de rede para restringir o acesso a serviços de rede ou aplicações, onde for necessário.

10.7 Manuseio de mídias

Objetivo: Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.

Convém que as mídias sejam controladas e fisicamente protegidas.

Convém que procedimentos operacionais apropriados sejam estabelecidos para proteger documentos, mídias magnéticas de computadores (fitas, discos), dados de entrada e saída e documentação dos sistemas contra divulgação não autorizada, modificação, remoção e destruição.

10.7.1 Gerenciamento de mídias removíveis

Controle
Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis.

Diretrizes para implementação
Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas:

a) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;

b) quando necessário e prático, seja requerida a autorização para remoção de qualquer mídia da organização e mantido o registro dessa remoção como trilha de auditoria;

c) toda mídia seja guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

d) informações armazenadas em mídias que precisam estar disponíveis por muito tempo (em conformidade com as especificações dos fabricantes) sejam também armazenadas em outro local para evitar perda de informações devido à deterioração das mídias;

e) as mídias removíveis sejam registradas para limitar a oportunidade de perda de dados;

f) as unidades de mídias removíveis estejam habilitadas somente se houver uma necessidade do negócio.

Convém que todos os procedimentos e os níveis de autorização sejam explicitamente documentados.

Informações adicionais
Mídia removível inclui fitas, discos, *flash disks*, discos removíveis, CD, DVD e mídia impressa.

10.7.2 Descarte de mídias

Controle
Convém que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.

Diretrizes para implementação
Convém que procedimentos formais para o descarte seguro das mídias sejam definidos para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas. Convém que os procedimentos para o descarte seguro das mídias, contendo informações sensíveis, sejam relativos à sensibilidade das informações. Convém que os seguintes itens sejam considerados:

a) mídias contendo informações sensíveis sejam guardadas e destruídas de forma segura e protegida, como, por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por uma outra aplicação dentro da organização;

b) procedimentos sejam implementados para identificar os itens que requerem descarte seguro;

c) pode ser mais fácil implementar a coleta e descarte seguro de todas as mídias a serem inutilizadas do que tentar separar apenas aquelas contendo informações sensíveis;

d) muitas organizações oferecem serviços de coleta e descarte de papel, de equipamentos e de mídias magnéticas; convém que se tenha o cuidado na seleção de um fornecedor com experiência e controles adequados;

e) descarte de itens sensíveis seja registrado em controles sempre que possível para se manter uma trilha de auditoria.

Quando da acumulação de mídias para descarte, convém que se leve em consideração o efeito proveniente do acúmulo, o que pode fazer com que uma grande quantidade de informação não sensível torne-se sensível.

Informações adicionais
Informações sensíveis podem ser divulgadas através do descarte negligente das mídias (ver 9.2.6 para informações de descarte de equipamentos).

10.7.3 Procedimentos para tratamento de informação

Controle
Convém que sejam estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido.

Diretrizes para implementação
Convém que procedimentos sejam estabelecidos para o tratamento, processamento, armazenamento e transmissão da informação, de acordo com a sua classificação (ver 7.2). Convém que os seguintes itens sejam considerados:

a) tratamento e identificação de todos os meios magnéticos indicando o nível de classificação;

b) restrições de acesso para prevenir o acesso de pessoas não autorizadas;

c) manutenção de um registro formal dos destinatários de dados autorizados;

d) garantia de que a entrada de dados seja completa, de que o processamento esteja devidamente concluído e de que a validação das saídas seja aplicada;

e) proteção dos dados preparados para expedição ou impressão de forma consistente com a sua criticidade;

f) armazenamento das mídias em conformidade com as especificações dos fabricantes;

g) manutenção da distribuição de dados no menor nível possível;

h) identificação eficaz de todas as cópias das mídias, para chamar a atenção dos destinatários autorizados;

i) análise crítica das listas de distribuição e das listas de destinatários autorizados em intervalos regulares.

Informações adicionais
Estes procedimentos são aplicados para informações em documentos, sistemas de computadores, redes de computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços postais, uso de máquinas de fax e qualquer outro item sensível, como, por exemplo, cheques em branco e faturas.

10.7.4 Segurança da documentação dos sistemas

Controle
Convém que a documentação dos sistemas seja protegida contra acessos não autorizados.

Diretrizes para implementação
Para proteger a documentação dos sistemas, convém que os seguintes itens sejam considerados:

a) a documentação dos sistemas seja guardada de forma segura;

b) a relação de pessoas com acesso autorizado à documentação de sistemas seja a menor possível e autorizada pelo proprietário do sistema;

c) a documentação de sistema mantida em uma rede pública, ou fornecida através de uma rede pública, seja protegida de forma apropriada.

Informações adicionais
A documentação dos sistemas pode conter uma série de informações sensíveis, como, por exemplo, descrições de processos da aplicação, procedimentos, estruturas de dados e processos de autorização.

10.8 Troca de informações

Objetivo: Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.

Convém que as trocas de informações e *softwares* entre organizações estejam baseadas numa política formal específica, sejam efetuadas a partir de acordos entre as partes e estejam em conformidade com toda a legislação pertinente (ver seção 15).

Convém que sejam estabelecidos procedimentos e normas para proteger a informação e a mídia física que contém informação em trânsito.

10.8.1 Políticas e procedimentos para troca de informações

Controle

Convém que políticas, procedimentos e controles sejam estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.

Diretrizes para implementação

Convém que os procedimentos e controles estabelecidos para a troca de informações em recursos eletrônicos de comunicação considerem os tópicos a seguir:

a) procedimentos formulados para proteger a informação em trânsito contra interceptação, cópia, modificação, desvio e destruição;

b) procedimentos para detecção e proteção contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação (ver 10.4.1);

c) procedimentos para proteção de informações eletrônicas sensíveis que sejam transmitidas na forma de anexos;

d) política ou diretrizes que especifiquem o uso aceitável dos recursos eletrônicos de comunicação (ver 7.1.3);

e) procedimentos para o uso de comunicação sem fio (*wireless*), levando em conta os riscos particulares envolvidos;

f) as responsabilidades de funcionários, fornecedores e quaisquer outros usuários não devem comprometer a organização através de, por exemplo, difamação, assédio, falsa identidade, retransmissão de "correntes", compras não autorizadas etc.;

g) uso de técnicas de criptografia para, por exemplo, proteger a confidencialidade, a integridade e a autenticidade das informações (ver 12.3);

h) diretrizes de retenção e descarte para toda a correspondência de negócios, incluindo mensagens, de acordo com regulamentações e legislação locais e nacionais relevantes;

i) não deixar informações críticas ou sensíveis em equipamentos de impressão, tais como copiadoras, impressoras e aparelhos de fax, de tal forma que pessoas não autorizadas tenham acesso a elas;

j) controles e restrições associados à retransmissão em recursos de comunicação como, por exemplo, a retransmissão automática de correios eletrônicos para endereços externos;

k) lembrar às pessoas que elas devem tomar precauções adequadas como, por exemplo, não revelar informações sensíveis, para evitar que sejam escutadas ou interceptadas durante uma ligação telefônica por:

   1) pessoas em sua vizinhança, especialmente quando estiver usando telefone celular;

   2) grampo telefônico e outras formas de escuta clandestina através do acesso físico ao aparelho telefônico ou à linha, ou, ainda, pelo uso de rastreadores;

   3) pessoas ao lado do interlocutor;

l) não deixar mensagens contendo informações sensíveis em secretárias eletrônicas, uma vez que as mensagens podem ser reproduzidas por pessoas não autorizadas, gravadas em sistemas públicos ou gravadas indevidamente por erro de discagem;

m) lembrar as pessoas sobre os problemas do uso de aparelhos de fax, tais como:

   1) acesso não autorizado a dispositivos para recuperação de mensagens;

   2) programação de aparelhos, deliberada ou acidental, para enviar mensagens para números específicos determinados;

   3) envio de documentos e mensagens para número errado, seja por falha na discagem ou uso de número armazenado errado;

n) lembrar as pessoas para que evitem o armazenamento de dados pessoais, como endereços de correios eletrônicos ou informações adicionais particulares, em qualquer *software*, impedindo que sejam capturados para uso não autorizado;

o) lembrar as pessoas sobre a existência de aparelhos de fax e copiadoras que têm dispositivos de armazenamento temporário de páginas para o caso de falha no papel ou na transmissão, as quais serão impressas após a correção da falha.

Adicionalmente, convém que as pessoas sejam lembradas de que não devem manter conversas confidenciais em locais públicos, escritórios abertos ou locais de reunião que não disponham de paredes à prova de som.

Convém que os recursos utilizados para a troca de informações estejam de acordo com os requisitos legais pertinentes (ver seção 15).

Informações adicionais
A troca de informações pode ocorrer através do uso de vários tipos diferentes de recursos de comunicação, incluindo correios eletrônicos, voz, fax e vídeo.

A troca de *softwares* pode ocorrer de diferentes formas, incluindo a baixa (*download*) da internet ou a aquisição junto a fornecedores que vendem produtos em série.

Convém que sejam consideradas as possíveis implicações nos negócios, nos aspectos legais e na segurança, relacionadas com a troca eletrônica de dados, com o comércio eletrônico, comunicação eletrônica e com os requisitos para controles.

As informações podem ser comprometidas devido à falta de conscientização, de políticas ou de procedimentos no uso de recursos de troca de informações, como, por exemplo, a escuta de conversas ao telefone celular em locais públicos, erro de endereçamento de mensagens de correio eletrônico, escuta não autorizada de mensagens gravadas em secretárias eletrônicas, acesso não autorizado a sistemas de correio de voz ou o envio acidental de faxes para aparelhos errados.

As operações do negócio podem ser prejudicadas e as informações podem ser comprometidas se os recursos de comunicação falharem, forem sobrecarregados ou interrompidos (ver 10.3 e seção 14). As informações podem ser comprometidas se acessadas por usuários não autorizados (ver seção 11).

10.8.2 Acordos para a troca de informações

Controle
Convém que sejam estabelecidos acordos para a troca de informações e *softwares* entre a organização e entidades externas.

Diretrizes para implementação
Convém que os acordos de troca de informações considerem as seguintes condições de segurança da informação:

a) responsabilidades do gestor pelo controle e notificação de transmissões, expedições e recepções;

b) procedimentos para notificar o emissor da transmissão, expedição e recepção;

c) procedimentos para assegurar a rastreabilidade dos eventos e o não-repúdio;

d) padrões técnicos mínimos para embalagem e transmissão;

e) acordos para procedimentos de custódia;

f) normas para identificação de portadores;

g) responsabilidades e obrigações na ocorrência de incidentes de segurança da informação, como perda de dados;

h) utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que o significado dos rótulos seja imediatamente entendido e que a informação esteja devidamente protegida;

i) propriedade e responsabilidades sobre a proteção dos dados, direitos de propriedade, conformidade com as licenças dos *softwares* e considerações afins (ver 15.1.2 e 15.1.4);

j) normas técnicas para a gravação e leitura de informações e *softwares*;

k) quaisquer controles especiais que possam ser necessários para proteção de itens sensíveis, tais como chaves criptográficas (ver 12.3).

Convém que políticas, procedimentos e normas para proteger as informações e as mídias em trânsito (ver também 10.8.3) sejam estabelecidos e mantidos, além de serem referenciados nos mencionados acordos para a troca de informações.

Convém que os aspectos de segurança contidos nos acordos reflitam a sensibilidade das informações envolvidas no negócio.

Informações adicionais
Os acordos podem ser eletrônicos ou manuais, e podem estar no formato de contratos formais ou condições de contratação. Para informações sensíveis, convém que os mecanismos específicos usados para a troca de tais informações sejam consistentes com todas as organizações e tipos de acordos.

10.8.3 Mídias em trânsito

Controle
Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.

Diretrizes para implementação
Convém que as seguintes recomendações sejam consideradas, para proteger as mídias que são transportadas entre localidades:

a) meio de transporte ou o serviço de mensageiros sejam confiáveis;

b) seja definida uma relação de portadores autorizados em concordância com o gestor;

c) sejam estabelecidos procedimentos para a verificação da identificação dos transportadores;

d) a embalagem seja suficiente para proteger o conteúdo contra qualquer dano físico, como os que podem ocorrer durante o transporte, e que seja feita de acordo com as especificações dos fabricantes (como no caso de *softwares*), por exemplo, protegendo contra fatores ambientais que possam reduzir a possibilidade de restauração dos dados como a exposição ao calor, umidade ou campos eletromagnéticos;

e) sejam adotados controles, onde necessário, para proteger informações sensíveis contra divulgação não autorizada ou modificação; como exemplo, pode-se incluir o seguinte:

   1) utilização de recipientes lacrados;

   2) entrega em mãos;

   3) lacre explícito de pacotes (que revele qualquer tentativa de acesso);

   4) em casos excepcionais, divisão do conteúdo em mais de uma remessa e expedição por rotas distintas.

Informações adicionais
As informações podem estar vulneráveis a acesso não autorizado, uso impróprio ou alteração indevida durante o transporte físico, por exemplo quando a mídia é enviada por via postal ou sistema de mensageiros.

10.8.4 Mensagens eletrônicas

Controle
Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

Diretrizes para implementação
Convém que as considerações de segurança da informação sobre as mensagens eletrônicas incluam o seguinte:

a) proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço;

b) assegurar que o endereçamento e o transporte da mensagem estejam corretos;

c) confiabilidade e disponibilidade geral do serviço;

d) aspectos legais, como, por exemplo, requisitos de assinaturas eletrônicas;

e) aprovação prévia para o uso de serviços públicos externos, tais como sistemas de mensagens instantâneas e compartilhamento de arquivos;

f) níveis mais altos de autenticação para controlar o acesso a partir de redes públicas.

Informações adicionais
Mensagens eletrônicas como correio eletrônico, *Eletronic Data Interchange* (EDI) e sistemas de mensagens instantâneas cumprem um papel cada vez mais importante nas comunicações do negócio. A mensagem eletrônica tem riscos diferentes, se comparada com a comunicação em documentos impressos.

10.8.5 Sistemas de informações do negócio

Controle
Convém que políticas e procedimentos sejam desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.

Diretrizes para implementação
Convém que as considerações sobre segurança da informação e implicações no negócio das interconexões de sistemas incluam o seguinte:

a) vulnerabilidades conhecidas nos sistemas administrativos e contábeis onde as informações são compartilhadas com diferentes áreas da organização;

b) vulnerabilidades da informação nos sistemas de comunicação do negócio, como, por exemplo, gravação de chamadas telefônicas ou teleconferências, confidencialidade das chamadas, armazenamento de faxes, abertura de correio e distribuição de correspondência;

c) política e controles apropriados para gerenciar o compartilhamento de informações;

d) exclusão de categorias de informações sensíveis e documentos confidenciais, caso o sistema não forneça o nível de proteção apropriado (ver 7.2);

e) restrição do acesso a informações de trabalho relacionado com indivíduos específicos, como, por exemplo, um grupo que trabalha com projetos sensíveis;

f) categorias de pessoas, fornecedores ou parceiros nos negócios autorizados a usar o sistema e as localidades a partir das quais pode-se obter acesso ao sistema (ver 6.2 e 6.3);

g) restrição aos recursos selecionados para categorias específicas de usuários;

h) identificação da condição do usuário, como, por exemplo,funcionários da organização ou fornecedores na lista de catálogo de usuários em benefício de outros usuários;

i) retenção e cópias de segurança das informações mantidas no sistema (ver 10.5.1);

j) requisitos e procedimentos para recuperação e contingência (ver seção 14).

Informações adicionais
Os sistemas de informação de escritório representam uma oportunidade de rápida disseminação e compartilhamento de informações do negócio através do uso de uma combinação de: documentos, computadores, dispositivos móveis, comunicação sem fio, correio, correio de voz, comunicação de voz em geral, multimídia, serviços postais e aparelhos de fax.

10.9 Serviços de comércio eletrônico

Objetivo: Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.

Convém que as implicações de segurança da informação associadas com o uso de serviços de comércio eletrônico, incluindo transações *on-line* e os requisitos de controle, sejam consideradas. Convém que a integridade e a disponibilidade da informação publicada eletronicamente por sistemas publicamente disponíveis sejam também consideradas.

10.9.1 Comércio eletrônico

Controle

Convém que as informações envolvidas em comércio eletrônico transitando sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

Diretrizes para implementação

Convém que as considerações de segurança da informação para comércio eletrônico incluam os seguintes itens:

a) nível de confiança que cada parte requer na suposta identidade de outros, como, por exemplo, por meio de mecanismos de autenticação;

b) processos de autorização com quem pode determinar preços, emitir ou assinar documentos-chave de negociação;

c) garantia de que parceiros comerciais estão completamente informados de suas autorizações;

d) determinar e atender requisitos de confidencialidade, integridade, evidências de emissão e recebimento de documentos-chave, e a não-repudiação de contratos, como, por exemplo, os associados aos processos de licitações e contratações;

e) nível de confiança requerido na integridade das listas de preços anunciadas;

f) a confidencialidade de quaisquer dados ou informações sensíveis;

g) a confidencialidade e integridade de quaisquer transações de pedidos, informações de pagamento, detalhes de endereço de entrega e confirmações de recebimentos;

h) grau de investigação apropriado para a verificação de informações de pagamento fornecidas por um cliente;

i) seleção das formas mais apropriadas de pagamento para proteção contra fraudes;

j) nível de proteção requerida para manter a confidencialidade e integridade das informações de pedidos;

k) prevenção contra perda ou duplicação de informação de transação;

l) responsabilidades associados com quaisquer transações fraudulentas;

m) requisitos de seguro.

Muitas das considerações acima podem ser endereçadas pela aplicação de controles criptográficos (ver 12.3), levando-se em conta a conformidade com os requisitos legais (ver 15.1, especialmente 15.1.6 para legislação sobre criptografia).

Convém que os procedimentos para comércio eletrônico entre parceiros comerciais sejam apoiados por um acordo formal que comprometa ambas as partes aos termos da transação, incluindo detalhes de autorização (ver b) acima). Outros acordos com fornecedores de serviços de informação e redes de valor agregado podem ser necessários.

Convém que sistemas comerciais públicos divulguem seus termos comerciais a seus clientes.

Convém que sejam consideradas a capacidade de resiliência dos servidores utilizados para comércio eletrônico contra ataques e as implicações de segurança de qualquer interconexão que seja necessária na rede de telecomunicações para a sua implementação (ver 11.4.6).

Informações adicionais
Comércio eletrônico é vulnerável a inúmeras ameaças de rede que podem resultar em atividades fraudulentas, disputas contratuais, e divulgação ou modificação de informação.

Comércio eletrônico pode utilizar métodos seguros de autenticação, como, por exemplo, criptografia de chave pública e assinaturas digitais (ver 12.3) para reduzir os riscos. Ainda, terceiros confiáveis podem ser utilizados onde tais serviços forem necessários.

10.9.2 Transações *on-line*

Controle
Convém que informações envolvidas em transações *on-line* sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

Diretrizes para implementação
Convém que as considerações de segurança para transações *on-line* incluam os seguintes itens:

a) uso de assinaturas eletrônicas para cada uma das partes envolvidas na transação;

b) todos os aspectos da transação, ou seja, garantindo que:

   1) credenciais de usuário para todas as partes são válidas e verificadas;

   2) a transação permaneça confidencial; e

   3) a privacidade de todas as partes envolvidas seja mantida;

c) caminho de comunicação entre todas as partes envolvidas é criptografado;

d) protocolos usados para comunicações entre todas as partes envolvidas é seguro;

e) garantir que o armazenamento dos detalhes da transação está localizado fora de qualquer ambiente publicamente acessível, como por exemplo, numa plataforma de armazenamento na intranet da organização, e não retida e exposta em um dispositivo de armazenamento diretamente acessível pela internet;

f) onde uma autoridade confiável é utilizada (como, por exemplo, para propósitos de emissão e manutenção de assinaturas e/ou certificados digitais), segurança é integrada a todo o processo de gerenciamento de certificados/assinaturas.

Informações adicionais
A extensão dos controles adotados precisará ser proporcional ao nível de risco associado a cada forma de transação *on-line.*

Transações podem precisar estar de acordo com leis, regras e regulamentações na jurisdição em que a transação é gerada, processada, completa ou armazenada.

Existem muitas formas de transações que podem ser executadas de forma *on-line,* como, por exemplo, contratuais, financeiras etc.

10.9.3 Informações publicamente disponíveis

Controle
Convém que a integridade das informações disponibilizadas em sistemas publicamente acessíveis seja protegida para prevenir modificações não autorizadas.

Diretrizes para implementação
Convém que aplicações, dados e informações adicionais que requeiram um alto nível de integridade e que sejam disponibilizados em sistemas publicamente acessíveis sejam protegidos por mecanismos apropriados, como, por exemplo, assinaturas digitais (ver 12.3). Convém que os sistemas acessíveis publicamente sejam testados contra fragilidades e falhas antes da informação estar disponível.

Convém que haja um processo formal de aprovação antes que uma informação seja publicada. Adicionalmente, convém que todo dado de entrada fornecido por fontes externas ao sistema seja verificado e aprovado.

Convém que sistemas de publicação eletrônica, especialmente os que permitem realimentação e entrada direta de informação, sejam cuidadosamente controlados, de forma que:

a) informações sejam obtidas em conformidade com qualquer legislação de proteção de dados (ver 15.1.4);

b) informações que sejam entradas e processadas por um sistema de publicação sejam processadas completa e corretamente em um tempo adequado;

c) informações sensíveis sejam protegidas durante a coleta, processamento e armazenamento;

d) acesso a sistemas de publicação não permita acesso não intencional a redes às quais tal sistema está conectado.

Informações adicionais
Informações em sistemas publicamente disponíveis, como, por exemplo, informações em servidores *web* acessíveis por meio da internet, podem necessitar estar de acordo com leis, regras e regulamentações na jurisdição em que o sistema está localizado, onde a transação está ocorrendo ou onde o proprietário reside. Modificações não autorizadas de informações publicadas podem trazer prejuízos à reputação da organização que a publica.

10.10 Monitoramento

Objetivo: Detectar atividades não autorizadas de processamento da informação.

Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados.

Convém que registros (*log*) de operador e registros (*log*) de falhas sejam utilizados para assegurar que os problemas de sistemas de informação são identificados.

Convém que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.

Convém que o monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

10.10.1 Registros de auditoria

Controle

Convém que registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

Diretrizes para implementação

Convém que os registros *(log)* de auditoria incluam, quando relevante:

a) identificação dos usuários;

b) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*log-on*) e saída (*log-off*) no sistema;

c) identidade do terminal ou, quando possível, a sua localização;

d) registros das tentativas de acesso ao sistema aceitas e rejeitadas;

e) registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;

f) alterações na configuração do sistema;

g) uso de privilégios;

h) uso de aplicações e utilitários do sistema;

i) arquivos acessados e tipo de acesso;

j) endereços e protocolos de rede;

k) alarmes provocados pelo sistema de controle de acesso;

l) ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus e sistemas de detecção de intrusos.

Informações adicionais

Os registros (*log*) de auditoria podem conter dados pessoais confidenciais e de intrusos. Convém que medidas apropriadas de proteção de privacidade sejam tomadas (ver 15.1.4). Quando possível, convém que administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (*log*) de suas próprias atividades (ver 10.1.3).

10.10.2 Monitoramento do uso do sistema

Controle

Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.

Diretrizes para implementação

Convém que o nível de monitoramento requerido para os recursos individuais seja determinado através de uma análise/avaliação de riscos. Convém que a organização esteja de acordo com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento. Convém que as seguintes áreas sejam consideradas:

a) acessos autorizados, incluindo detalhes do tipo:

   1) o identificador do usuário (ID de usuário);

   2) a data e o horário dos eventos-chave;

   3) tipo do evento;

   4) os arquivos acessados;

   5) os programas ou utilitários utilizados;

b) todas as operações privilegiadas, tais como:

   1) uso de contas privilegiadas, por exemplo: supervisor, *root*, administrador;

   2) inicialização e finalização do sistema;

   3) a conexão e a desconexão de dispositivos de entrada e saída;

c) tentativas de acesso não autorizadas, tais como:

   1) ações de usuários com falhas ou rejeitados;

   2) ações envolvendo dados ou outros recursos com falhas ou rejeitadas;

   3) violação de políticas de acesso e notificações para *gateways* de rede e *firewalls*;

   4) alertas dos sistemas proprietários de detecção de intrusos;

d) alertas e falhas do sistema, tais como:

   1) alertas ou mensagens do console;

   2) registro das exceções do sistema;

   3) alarmes do gerenciamento da rede;

   4) alarmes disparados pelo sistema de controle de acesso;

e) alterações ou tentativas de alterações nos controles e parâmetros dos sistemas de segurança.

Convém que a freqüência da análise crítica dos resultados das atividades de monitaramento dependa dos riscos envolvidos. Convém que os seguintes fatores de risco sejam considerados:

a) criticidade dos processos de aplicação;

b) valor, sensibilidade e criticidade da informação envolvida;

c) experiência anterior com infiltrações e uso impróprio do sistema e da freqüência das vulnerabilidades sendo exploradas;

d) extensão da interconexão dos sistemas (particularmente com redes públicas);

e) desativação da gravação dos registros (*logs*).

Informações adicionais
O uso de procedimentos de monitoramento é necessário para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas.

A análise crítica dos registros (*log*) envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual isto pode acontecer. Exemplos de eventos que podem requerer uma maior investigação em casos de incidentes de segurança da informação são comentados em 13.1.1.

10.10.3 Proteção das informações dos registros (*log)*

Controle
Convém que os recursos e informações de registros (*log*) sejam protegidos contra falsificação e acesso não autorizado.

Diretrizes para implementação
Convém que os controles implementados objetivem a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros (*log*), tais como:

a) alterações dos tipos de mensagens que são gravadas;

b) arquivos de registros (*log*) sendo editados ou excluídos;

c) capacidade de armazenamento da mídia magnética do arquivo de registros (*log*) excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

Alguns registros (*log*) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência (ver 13.2.3).

Informações adicionais
Registros (*log*) de sistema normalmente contêm um grande volume de informações e muitos dos quais não dizem respeito ao monitoramento da segurança. Para ajudar a identificar eventos significativos para propósito de monitoramento de segurança, convém que a cópia automática dos tipos de mensagens para a execução de consulta seja considerada e/ou o uso de sistemas utilitários adequados ou ferramentas de auditoria para realizar a racionalização e investigação do arquivo seja considerado.

Registros (*log*) de sistema precisam ser protegidos, pois os dados podem ser modificados e excluídos e suas ocorrências podem causar falsa impressão de segurança.

10.10.4 Registros (*log*) de administrador e operador

Controle
Convém que as atividades dos administradores e operadores do sistema sejam registradas.

Diretrizes para implementação
Convém que esses registros (*log*) incluam:

a) a hora em que o evento ocorreu (sucesso ou falha);

b) informações sobre o evento (exemplo: arquivos manuseados) ou falha (exemplo: erros ocorridos e ações corretivas adotadas);

c) que conta e que administrador ou operador estava envolvido;

d) que processos estavam envolvidos.

Convém que os registros (*log*) de atividades dos operadores e administradores dos sistemas sejam analisados criticamente em intervalos regulares.

Informações adicionais
Um sistema de detecção de intrusos gerenciado fora do controle dos administradores de rede e de sistemas pode ser utilizado para monitorar a conformidade das atividades dos administradores do sistema e da rede.

10.10.5 Registros (*log*) de falhas

Controle
Convém que as falhas ocorridas sejam registradas e analisadas, e que sejam adotadas ações apropriadas.

Diretrizes para implementação
Convém que falhas informadas pelos usuários ou pelos programas de sistema relacionado a problemas com processamento da informação ou sistemas de comunicação sejam registradas. Convém que existam regras claras para o tratamento das falhas informadas, incluindo:

a) análise crítica dos registros (*log*) de falha para assegurar que as falhas foram satisfatoriamente resolvidas;

b) análise crítica das medidas corretivas para assegurar que os controles não foram comprometidos e que a ação tomada é completamente autorizada.

Convém que seja assegurado que o registro de erros esteja habilitado, caso essa função do sistema esteja disponível.

Informações adicionais
Registros de falhas e erros podem impactar o desempenho do sistema. Convém que cada tipo de registro a ser coletado seja habilitado por pessoas competentes e que o nível de registro requerido para cada sistema individual seja determinado por uma análise/avaliação de riscos, levando em consideração a degradação do desempenho do sistema.

10.10.6 Sincronização dos relógios

Controle
Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma fonte de tempo precisa, acordada.

Diretrizes para implementação
Onde um computador ou dispositivo de comunicação tiver a capacidade para operar um relógio (*clock*) de tempo real, convém que o relógio seja ajustado conforme o padrão acordado, por exemplo o tempo coordenado universal (*Coordinated Universal Time - UTC*) ou um padrão de tempo local. Como alguns relógios são conhecidos pela sua variação durante o tempo, convém que exista um procedimento que verifique esses tipos de inconsistências e corrija qualquer variação significativa.

A interpretação correta do formato data/hora é importante para assegurar que o *timestamp* reflete a data/hora real. Convém que se levem em conta especificações locais (por exemplo, horário de verão).

Informações adicionais
O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros (*log*) de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros (*log*) de auditoria incorretos podem impedir tais investigações e causar danos à credibilidade das evidências. Um relógio interno ligado ao relógio atômico nacional via transmissão de rádio pode ser utilizado como relógio principal para os sistemas de registros (*logging*). O protocolo de hora da rede pode ser utilizado para sincronizar todos os relógios dos servidores com o relógio principal.

11 Controle de acessos

11.1 Requisitos de negócio para controle de acesso

Objetivo: Controlar acesso à informação.

Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.

Convém que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação.

11.1.1 Política de controle de acesso

Controle
Convém que a política de controle de acesso seja estabelecida documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.

Diretrizes para implementação
Convém que as regras de controle de acesso e direitos para cada usuário ou grupos de usuários sejam expressas claramente na política de controle de acesso. Convém considerar os controles de acesso lógico e físico (ver seção 9) de forma conjunta. Convém fornecer aos usuários e provedores de serviços uma declaração nítida dos requisitos do negócio a serem atendidos pelos controles de acessos.

Convém que a política leve em consideração os seguintes itens:

a) requisitos de segurança de aplicações de negócios individuais;

b) identificação de todas as informações relacionadas às aplicações de negócios e os riscos a que as informações estão expostas;

c) política para disseminação e autorização da informação, por exemplo, o princípio *need to know* e níveis de segurança e a classificação das informações (ver 7.2);

d) consistência entre controle de acesso e políticas de classificação da informação em diferentes sistemas e redes;

e) legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços (ver 15.1);

f) perfis de acesso de usuário-padrão para trabalhos comuns na organização;

g) administração de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;

h) segregação de funções para controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;

i) requisitos para autorização formal de pedidos de acesso (ver 11.2.1);

j) requisitos para análise crítica periódica de controles de acesso (ver 11.2.4);

k) remoção de direitos de acesso (ver 8.3.3).

Informações adicionais
Convém que sejam tomados cuidados na especificação de regras de controle de acesso quando se considerar o seguinte:

a) diferenciar entre regras que devem ser obrigatórias e forçadas, e diretrizes que são opcionais ou condicionais;

b) estabelecer regra baseada na premissa "Tudo é proibido, a menos que expressamente permitido" em lugar da regra mais fraca "Tudo é permitido, a menos que expressamente proibido";

c) mudanças em rótulos de informação (ver 7.2) que são iniciadas automaticamente através de recursos de processamento da informação e os que iniciaram pela ponderação de um usuário;

d) mudanças em permissões de usuário que são iniciadas automaticamente pelo sistema de informação e aqueles iniciados por um administrador;

e) regras que requerem aprovação específica antes de um decreto ou lei e as que não necessitam.

Convém que as regras para controle de acesso sejam apoiadas por procedimentos formais e responsabilidades claramente definidas (ver 6.1.3, 11.3, 10.4.1 e 11.6).

11.2 Gerenciamento de acesso do usuário

Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.

Convém que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

Convém que os procedimentos cubram todas as fases do ciclo de vida de acesso do usuário, da inscrição inicial como novos usuários até o cancelamento final do registro de usuários que já não requerem acesso a sistemas de informação e serviços. Convém que atenção especial seja dada, onde apropriado, para a necessidade de controlar a distribuição de direitos de acesso privilegiado que permitem os usuários mudar controles de sistemas.

11.2.1 Registro de usuário

Controle
Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.

Diretrizes para implementação
Convém que os procedimentos de controle de acesso para registro e cancelamento de usuários incluam:

a) utilizar identificador de usuário (ID de usuário) único para assegurar a responsabilidade de cada usuário por suas ações; convém que o uso de grupos de ID somente seja permitido onde existe a necessidade para o negócio ou por razões operacionais, e isso seja aprovado e documentado;

b) verificar se o usuário tem autorização do proprietário do sistema para o uso do sistema de informação ou serviço; aprovação separada para direitos de acesso do gestor também pode ser apropriada;

c) verificar se o nível de acesso concedido é apropriado ao propósito do negócio (ver 11.1) e é consistente com a política de segurança da organização, por exemplo, não compromete a segregação de função (ver 10.1.3);

d) dar para os usuários uma declaração por escrito dos seus direitos de acesso;

e) requerer aos usuários a assinatura de uma declaração indicando que eles entendem as condições de acesso;

f) assegurar aos provedores de serviços que não serão dados acessos até que os procedimentos de autorização tenham sido concluídos;

g) manter um registro formal de todas as pessoas registradas para usar o serviço;

h) remover imediatamente ou bloquear direitos de acesso de usuários que mudaram de cargos ou funções, ou deixaram a organização;

i) verificar periodicamente e remover ou bloquear identificadores (ID) e contas de usuário redundantes (ver 11.2.4);

j) assegurar que identificadores de usuário (ID de usuário) redundantes não sejam atribuídos para outros usuários.

Informações adicionais
Convém que seja considerado estabelecer perfis de acesso do usuário baseados nos requisitos dos negócios que resumam um número de direitos de acessos dentro de um perfil de acesso típico de usuário. Solicitações de acessos e análises críticas (ver 11.2.4) são mais fáceis de gerenciar ao nível de tais perfis do que ao nível de direitos particulares.

Convém que seja considerada a inclusão de cláusulas nos contratos de usuários e de serviços que especifiquem as sanções em caso de tentativa de acesso não autorizado pelos usuários ou por terceiros (ver 6.1.5, 8.1.3 e 8.2.3).

11.2.2 Gerenciamento de privilégios

Controle
Convém que a concessão e o uso de privilégios sejam restritos e controlados.

Diretrizes para implementação
Convém que os sistemas de multiusuários que necessitam de proteção contra acesso não autorizado tenham a concessão de privilégios controlada por um processo de autorização formal. Convém que os seguintes passos sejam considerados:

a) privilégio de acesso de cada produto de sistema, por exemplo, sistema operacional, sistemas de gerenciamento de banco de dados e cada aplicação, e de categorias de usuários para os quais estes necessitam ser concedido, seja identificado;

b) os privilégios sejam concedidos a usuários conforme a necessidade de uso e com base em eventos alinhados com a política de controle de acesso (ver 11.1.1), por exemplo, requisitos mínimos para sua função somente quando necessário;

c) um processo de autorização e um registro de todos os privilégios concedidos sejam mantidos. Convém que os privilégios não sejam fornecidos até que todo o processo de autorização esteja finalizado;

d) desenvolvimento e uso de rotinas de sistemas sejam incentivados de forma a evitar a necessidade de fornecer privilégios aos usuários;

e) desenvolvimento e uso de programas que não necessitam funcionar com privilégios sejam estimulados;

f) os privilégios sejam atribuídos para um identificador de usuário (ID de usuário) diferente daqueles usados normalmente para os negócios.

Informações adicionais
O uso inapropriado de privilégios de administrador de sistemas (qualquer característica ou recursos de sistemas de informação que habilitam usuários a exceder o controle de sistemas ou aplicações) pode ser um grande fator de contribuição para falhas ou violações de sistemas.

11.2.3 Gerenciamento de senha do usuário

Controle
Convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal.

Diretrizes para implementação
Convém que o processo considere os seguintes requisitos:

a) solicitar aos usuários a assinatura de uma declaração, para manter a confidencialidade de sua senha pessoal e das senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições da contratação (ver 8.1.3);

b) garantir, onde os usuários necessitam manter suas próprias senhas, que sejam fornecidas inicialmente senhas seguras e temporárias (ver 11.3.1), o que obriga o usuário a alterá-la imediatamente;

c) estabelecer procedimentos para verificar a identidade de um usuário antes de fornecer uma senha temporária, de substituição ou nova;

d) fornecer senhas temporárias aos usuários de maneira segura; convém que o uso de mensagens de correio eletrônico de terceiros ou desprotegido (texto claro) seja evitado;

e) senhas temporárias sejam únicas para uma pessoa e não sejam fáceis de serem adivinhadas;

f) usuários acusem o recebimento de senhas;

g) as senhas nunca sejam armazenadas nos sistemas de um computador de forma desprotegida;

h) as senhas padrão sejam alteradas logo após a instalação de sistemas ou *software*.

Informações adicionais
Senhas são um meio comum de verificar a identidade de um usuário antes que acessos sejam concedidos a um sistema de informação ou serviço de acordo com a autorização do usuário. Outras tecnologias para identificação de usuário e autenticação, como biométrica, por exemplo, verificação de digitais, verificação de assinatura, e uso de *tokens*, por exemplo, e cartões inteligentes, estão disponíveis, e convém que sejam consideradas, se apropriado.

11.2.4 Análise crítica dos direitos de acesso de usuário

Controle
Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

Diretrizes para implementação
Convém que a análise crítica dos direitos de acesso considere as seguintes orientações:

a) os direitos de acesso de usuários sejam revisados em intervalos regulares, por exemplo, um período de seis meses e depois de qualquer mudança, como promoção, rebaixamento ou encerramento do contrato (ver 11.2.1);

b) os direitos de acesso de usuários sejam analisados criticamente e realocados quando movidos de um tipo de atividade para outra na mesma organização;

c) autorizações para direitos de acesso privilegiado especial (ver 11.2.2) sejam analisadas criticamente em intervalos mais freqüentes, por exemplo, em um período de três meses;

d) as alocações de privilégios sejam verificadas em intervalo de tempo regular para garantir que privilégios não autorizados não foram obtidos;

e) as modificações para contas de privilégios sejam registradas para análise crítica periódica.

Informações adicionais
É necessário analisar criticamente, a intervalos regulares, os direitos de acesso de usuários para manter o controle efetivo sobre os acessos de dados e serviços de informação.

11.3 Responsabilidades dos usuários

Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

A cooperação de usuários autorizados é essencial para uma efetiva segurança.

Convém que os usuários estejam conscientes de suas responsabilidades para manter efetivo controle de acesso, particularmente em relação ao uso de senhas e de segurança dos equipamentos de usuários.

Convém que uma política de mesa e tela limpa seja implementada para reduzir o risco de acessos não autorizados ou danos a documentos/papéis, mídias e recursos de processamento da informação.

11.3.1 Uso de senhas

Controle
Convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas.

Diretrizes para implementação
Convém que todos os usuários sejam informados para:

a) manter a confidencialidade das senhas;

b) evitar manter anotadas senhas (por exemplo, papel, arquivos ou dispositivos móveis), a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado;

c) alterar senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

d) selecionar senhas de qualidade com um tamanho mínimo que sejam:

   1) fáceis de lembrar;

   2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;

   3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário);

   4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

e) modificar senhas regularmente ou com base no número de acessos (convém que senhas de acesso a contas privilegiadas sejam modificadas mais freqüentemente que senhas normais) e evitar a reutilização ou reutilização do ciclo de senhas antigas;

f) modificar senhas temporárias no primeiro acesso ao sistema;

g) não incluir senhas em nenhum processo automático de acesso ao sistema, por exemplo, armazenadas em um macro ou funções-chave;

h) não compartilhar senhas de usuários individuais;

i) não utilizar a mesma senha para uso com finalidades profissionais e pessoais.

Se os usuários necessitam acessar múltiplos serviços, sistemas ou plataformas, e forem requeridos para manter separadamente múltiplas senhas, convém que eles sejam alertados para usar uma única senha de qualidade (ver d) acima) para todos os serviços, já que o usuário estará assegurado de que um razoável nível de proteção foi estabelecido para o armazenamento da senha em cada serviço, sistema ou plataforma.

Informações adicionais
A gestão do sistema de *help desk* que trata de senhas perdidas ou esquecidas necessita de cuidado especial, pois este caminho pode ser também um dos meios de ataque ao sistema de senha.

11.3.2 Equipamento de usuário sem monitoração

Controle
Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

Diretrizes para implementação
Convém que todos os usuários estejam cientes dos requisitos de segurança da informação e procedimentos para proteger equipamentos desacompanhados, assim como suas responsabilidades por implementar estas proteções. Convém que os usuários sejam informados para:

a) encerrar as sessões ativas,a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio, por exemplo tela de proteção com senha;

b) efetuar a desconexão com o computador de grande porte, servidores e computadores pessoais do escritório, quando a sessão for finalizada (por exemplo: não apenas desligar a tela do computador ou o terminal);

c) proteger os microcomputadores ou terminais contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo, senha de acesso, quando não estiver em uso (ver 11.3.3).

Informações adicionais
Equipamentos instalados em áreas de usuários, por exemplo, estações de trabalho ou servidores de arquivos, podem requerer proteção especial contra acesso não autorizado, quando deixados sem monitoração por um período extenso.

11.3.3 Política de mesa limpa e tela limpa

Controle
Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação.

Diretrizes para implementação
Convém que uma política de mesa limpa e tela limpa leve em consideração a classificação da informação (ver 7.2), requisitos contratuais e legais (ver 15.1), e o risco correspondente e aspectos culturais da organização. Convém que as seguintes diretrizes sejam consideradas:

a) informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

b) computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, *token* ou mecanismo de autenticação similar quando sem monitoração e protegidos por tecla de bloqueio, senhas ou outros controles, quando não usados;

c) pontos de entrada e saída de correspondências e máquinas de fac-símile sem monitoração sejam protegidos;

d) sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, *scanners*, máquinas fotográficas digitais);

e) documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

Informações adicionais
Uma política de mesa limpa e tela limpa reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

Considerar o uso de impressoras com função de código PIN, permitindo desta forma que os requerentes sejam os únicos que possam pegar suas impressões, e apenas quando estiverem próximos às impressoras.

11.4 Controle de acesso à rede

Objetivo: Prevenir acesso não autorizado aos serviços de rede.

Convém que o acesso aos serviços de rede internos e externos seja controlado.

Convém que os usuários com acesso às redes e aos serviços de rede não comprometam a segurança desses serviços, assegurando:

a) uso de interfaces apropriadas entre a rede da organização e as redes de outras organizações e redes públicas;

b) uso de mecanismos de autenticação apropriados para os usuários e equipamentos;

c) controle de acesso compulsório de usuários aos serviços de informação.

11.4.1 Política de uso dos serviços de rede

Controle
Convém que usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.

Diretrizes para implementação
Convém que uma política seja formulada relativamente ao uso de redes e serviços de rede. Convém que esta política cubra:

a) redes e serviços de redes que são permitidos de serem acessados;

b) procedimentos de autorização para determinar quem tem permissão para acessar em quais redes e serviços de redes;

c) procedimentos e controles de gerenciamento para proteger acesso a conexões e serviços de redes;

d) os meios usados para acessar redes e serviços de rede (por exemplo, as condições por permitir acesso discado para acessar o provedor de serviço internet ou sistema remoto).

Convém que a política no uso de serviços de rede seja consistente com a política de controle de acesso do negócio (ver 11.1).

Informações adicionais
Conexões sem autorização e inseguras nos serviços de rede podem afetar toda organização. Este controle é particularmente importante para conexões de redes sensíveis ou aplicações de negócios críticos ou para usuários em locais de alto risco, por exemplo, áreas públicas ou externas que estão fora da administração e controle da segurança da organização.

11.4.2 Autenticação para conexão externa do usuário

Controle
Convém que métodos apropriados de autenticações sejam usados para controlar acesso de usuários remotos.

Diretrizes para implementação
A autenticação de usuários remotos pode ser alcançada usando, por exemplo, técnica baseada em criptografia, *hardware tokens* ou um protocolo de desafio/resposta. Podem ser achadas possíveis implementações de tais técnicas em várias soluções de redes privadas virtuais (VPN). Também podem ser usadas linhas privadas dedicadas para prover garantia da origem de conexões.

Os procedimentos e controles de discagem reversa (*dial-back*), por exemplo, usando modens com discagem reversa, podem prover proteção contra conexões não autorizadas e não desejadas nos recursos de processamento da informação de uma organização. Este tipo de controle autentica usuários que tentam estabelecer conexões com a rede de uma organizações de localidades remotas. Ao usar este controle, convém que uma organização não use serviços de rede que incluem transferência de chamadas (*forward*) ou, se eles fizerem, convém que seja desabilitado o uso de tais facilidades para evitar exposição a fragilidades associadas ao *call forward*. Convém que o processo de discagem reversa assegure que uma desconexão atual no lado da organização aconteça. Caso contrário, o usuário remoto poderia reter aberta a linha simulando que a verificação do retorno da chamada (*call back*) ocorreu. Convém que os procedimentos e controles da discagem reversa sejam testados completamente para esta possibilidade.

Autenticação de um nó pode servir como meio alternativo de autenticar grupos de usuários remotos onde eles são conectados a recursos de computador seguros e compartilhados. Técnicas criptográficas, por exemplo, com base em certificados de máquina, podem ser usadas para autenticação de nó. Isto é parte de várias soluções baseado em VPN.

Convém que seja implementado controle de autenticação adicional para controlar acesso a redes sem fios. Em particular, cuidado especial é necessário na seleção de controles para redes sem fios devido às numerosas oportunidades de não detecção de interceptação e inserção de tráfico de rede.

Informações adicionais
As conexões externas proporcionam um potencial de acessos não autorizados para as informações de negócio, por exemplo, acesso por métodos discados (*dial-up*). Existem diferentes tipos de métodos de autenticação, alguns deles proporcionam um maior nível de proteção que outros, por exemplo, métodos baseados em técnicas de criptografia que podem proporcionar autenticação forte. É importante determinar o nível de proteção requerido a partir de uma análise/avaliação de riscos. Isto é necessário para selecionar apropriadamente um método de autenticação.

Os recursos de conexão automática para computadores remotos podem prover um caminho para ganhar acesso não autorizado nas aplicações de negócio. Isto é particularmente importante se a conexão usar uma rede que está fora do controle do gerenciamento de segurança da informação da organização.

11.4.3 Identificação de equipamento em redes

Controle
Convém que sejam consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.

Diretrizes para implementação
Uma identificação de equipamentos pode ser usada se for importante que a comunicação possa somente ser iniciada de um local ou equipamento específico. Um identificador no equipamento pode ser usado para indicar se este equipamento possui permissão para conectar-se à rede. Convém que estes identificadores indiquem claramente para qual rede o equipamento possui permissão para conectar-se, se existe mais de uma rede e particularmente se estas redes são de sensibilidade diferente. Pode ser necessário considerar proteção física do equipamento para manter a segurança do identificador do equipamento.

Informações adicionais
Este controle pode ser complementado com outras técnicas para autenticar o usuário do equipamento (ver 11.4.2). Pode ser aplicada identificação de equipamento adicionalmente à autenticação de usuário.

11.4.4 Proteção de portas de configuração e diagnóstico remotos

Controle
Convém que sejam controlados os acessos físico e lógico a portas de diagnóstico e configuração.

Diretrizes para implementação
Os controles potenciais para o acesso às portas de diagnóstico e configuração incluem o uso de uma tecla de bloqueio e procedimentos de suporte para controlar o acesso físico às portas. Um exemplo para tal procedimento é assegurar que as portas de diagnóstico e configuração são apenas acessíveis pela combinação do acesso requerido entre o gestor dos serviços do computador e pelo pessoal de suporte do *hardware/software*.

Convém que portas, serviços e recursos similares instalados em um computador ou recurso de rede que não são especificamente requeridos para a funcionalidade do negócio sejam desabilitados ou removidos.

Informações adicionais
Muitos sistemas de computadores, sistemas de rede e sistemas de comunicação são instalados com os recursos de diagnóstico ou configuração remota para uso pelos engenheiros de manutenção. Se desprotegidas, estas portas de diagnóstico proporcionam meios de acesso não autorizado.

11.4.5 Segregação de redes

Controle
Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

Diretrizes para implementação
Um método de controlar a segurança da informação em grandes redes é dividir em diferentes domínios de redes lógicas, por exemplo, os domínios de redes internas de uma organização e domínios externos de uma rede, cada um protegido por um perímetro de segurança definido. Um conjunto de controles reguláveis pode ser aplicado em domínios de redes lógicas diferentes para adicionar mais segurança aos ambientes de segurança de rede, por exemplo, sistemas publicamente acessíveis, redes internas e ativos críticos. Convém que os domínios sejam definidos com base em uma análise/avaliação de riscos e os requisitos de segurança diferentes dentro de cada um dos domínios.

Tal perímetro de rede pode ser implementado instalando um *gateway* seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informação entre os dois domínios. Convém que este *gateway* seja configurado para filtrar tráfico entre estes domínios (ver 11.4.6 e 11.4.7) e bloquear acesso não autorizado conforme a política de controle de acesso da organização (ver 11.1). Um exemplo deste tipo de *gateway* é o que geralmente é chamado de *firewall*. Outro método de segregar domínios lógicos é restringir acesso de rede usando redes privadas virtuais para grupos de usuário dentro da organização.

Podem também ser segregadas redes usando a funcionalidade de dispositivo de rede, por exemplo, IP *switching*. Os domínios separados podem ser implementados controlando os fluxos de dados de rede, usando as capacidades de roteamento/chaveamento (*routing/switching)*, do mesmo modo que listas de controle de acesso.

Convém que critérios para segregação de redes em domínios estejam baseados na política de controle de acesso e requisitos de acesso (ver 10.1), e também levem em conta os custos relativos e impactos de desempenho em incorporar roteamento adequado à rede ou tecnologia de *gateway* (ver 11.4.6 e 11.4.7).

Além disso, convém que segregação de redes esteja baseada no valor e classificação de informações armazenadas ou processadas na rede, níveis de confiança ou linhas de negócio para reduzir o impacto total de uma interrupção de serviço.

Convém considerar à segregação de redes sem fios de redes internas e privadas. Como os perímetros de redes sem fios não são bem definidos, convém que uma análise/avaliação de riscos seja realizada em tais casos para identificar os controles (por exemplo, autenticação forte, métodos criptográficos e seleção de freqüência) para manter segregação de rede.

Informações adicionais
As redes estão sendo progressivamente estendidas além dos limites organizacionais tradicionais, tendo em vista as parcerias de negócio que são formadas e que podem requerer a interconexão ou compartilhamento de processamento de informação e recursos de rede. Tais extensões podem aumentar o risco de acesso não autorizado a sistemas de informação existentes que usam a rede e alguns dos quais podem requerer proteção de outros usuários de rede devido a sensibilidade ou criticidade.

11.4.6 Controle de conexão de rede

Controle
Para redes compartilhadas, especialmente essas que se estendem pelos limites da organização, convém que a capacidade dos usuários para conectar-se à rede seja restrita, alinhada com a política de controle de acesso e os requisitos das aplicações do negócio (ver 11.1).

Diretrizes para implementação
Convêm que os direitos de acesso dos usuários a rede sejam mantidos e atualizados conforme requerido pela política de controle de acesso (ver 11.1.1).

A capacidade de conexão de usuários pode ser restrita através dos *gateways* que filtram tráfico por meio de tabelas ou regras predefinidas. Convém que sejam aplicadas restrições nos seguintes exemplos de aplicações:

a) mensagens, por exemplo, correio eletrônico;

b) transferência de arquivo;

c) acesso interativo;

d) acesso à aplicação.

Convém que sejam considerados direitos de acesso entre redes para certo período do dia ou datas.

Informações adicionais
A incorporação de controles para restringir a capacidade de conexão dos usuários pode ser requerida pela política de controle de acesso para redes compartilhadas, especialmente aquelas que estendam os limites organizacionais.

11.4.7 Controle de roteamento de redes

Controle
Convém que seja implementado controle de roteamento na rede, para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.

Diretrizes para implementação
Convém que os controles de roteamento sejam baseados no mecanismo de verificação positiva do endereço de origem e destinos.

Os *gateways* de segurança podem ser usados para validar endereços de origem e destino nos pontos de controle de rede interna ou externa se o *proxy* e/ou a tecnologia de tradução de endereço forem empregados. Convém que os implementadores estejam conscientes da força e deficiências de qualquer mecanismo implementado. Convém que os requisitos de controles de roteamento das redes sejam baseados na política de controle de acesso (ver 11.1).

Informações adicionais
As redes compartilhadas, especialmente as que estendem os limites organizacionais, podem requerer controles adicionais de roteamento. Isto se aplica particularmente onde são compartilhadas redes com terceiros (usuários que não pertencem a organização).

11.5 Controle de acesso ao sistema operacional

Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.

Convém que recursos de segurança da informação sejam usados para restringir o acesso aos sistemas operacionais para usuários autorizados. Convém que estes recursos permitam:

a) autenticação de usuários autorizados, conforme a política de controle de acesso definida;

b) registro das tentativas de autenticação no sistema com sucesso ou falha;

c) registro do uso de privilégios especiais do sistema;

d) disparo de alarmes quando as políticas de segurança do sistema são violadas;

e) fornecer meios apropriados de autenticação;

f) restrição do tempo de conexão dos usuários, quando apropriado.

11.5.1 Procedimentos seguros de entrada no sistema (*log-on*)

Controle
Convém que o acesso aos sistemas operacionais seja controlado por um procedimento seguro de entrada no sistema (*log-on*).

Diretrizes para implementação
Convém que o procedimento para entrada no sistema operacional seja configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada (*log-on*) divulgue o mínimo de informações sobre o sistema, de forma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado. Convém que um bom procedimento de entrada no sistema (*log-on*):

a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso;

b) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;

c) não forneça mensagens de ajuda durante o procedimento de entrada (*log-on*) que poderiam auxiliar um usuário não autorizado;

d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, convém que o sistema não indique qual parte do dado de entrada está correta ou incorreta;

e) limite o número permitido de tentativas de entradas no sistema (*log-on*) sem sucesso, por exemplo, três tentativas, e considere:

   1) registro das tentativas com sucesso ou com falha;

   2) imposição do tempo de espera antes de permitir novas tentativas de entrada no sistema (*log-on*) ou rejeição de qualquer tentativa posterior de acesso sem autorização específica;

   3) encerramento das conexões por *data link*;

   4) envio de uma mensagem de alerta para o *console* do sistema, se o número máximo de tentativas de entrada no sistema (*log-on*) for alcançado;

   5) configuração do número de tentativas de senhas alinhado com o tamanho mínimo da senha e o valor do sistema que está sendo protegido;

f) limite o tempo máximo e mínimo permitido para o procedimento de entrada no sistema (*log-on*). Se excedido, convém que o sistema encerre o procedimento;

g) mostre as seguintes informações, quando o procedimento de entrada no sistema (*log-on*) finalizar com sucesso:

   1) data e hora da última entrada no sistema (*log-on*) com sucesso;

   2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (*log-on*) desde o último acesso com sucesso;

h) não mostre a senha que está sendo informada ou considere ocultar os caracteres da senha por símbolos;

i) não transmita senhas em texto claro pela rede.

Informações adicionais
Se as senhas forem transmitidas em texto claro durante o procedimento de entrada no sistema (*log-on*) pela rede, elas podem ser capturadas por um programa de *sniffer* de rede, instalado nela.

11.5.2 Identificação e autenticação de usuário

Controle
Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.

Diretrizes para implementação
Convém que este controle seja aplicado para todos os tipos de usuários (incluindo o pessoal de suporte técnico, operadores, administradores de rede, programadores de sistema e administradores de banco de dados).

Convém que os identificadores de usuários (ID de usuários) possam ser utilizados para rastrear atividades ao indivíduo responsável. Convém que atividades regulares de usuários não sejam executadas através de contas privilegiadas.

Em circunstâncias excepcionais, onde exista um claro benefício ao negócio, pode ocorrer a utilização de um identificador de usuário (ID de usuário) compartilhado por um grupo de usuários ou para um trabalho específico. Convém que a aprovação pelo gestor esteja documentada nestes casos. Controles adicionais podem ser necessários para manter as responsabilidades.

Convém que identificadores de usuários (ID de usuários) genéricos para uso de um indivíduo somente sejam permitidos onde as funções acessíveis ou as ações executadas pelo usuário não precisam ser rastreadas (por exemplo, acesso somente leitura), ou quando existem outros controles implementados (por exemplo, senha para identificador de usuário genérico somente fornecida para um indivíduo por vez e registrada).

Convém que onde autenticação forte e verificação de identidade é requerida, métodos alternativos de autenticação de senhas, como meios criptográficos, cartões inteligentes (*smart card*), *tokens* e meios biométricos sejam utilizados.

Informações adicionais
As senhas (ver 11.3.1 e 11.5.3) são uma maneira muito comum de se prover identificação e autenticação com base em um segredo que apenas o usuário conhece. O mesmo pode ser obtido com meios criptográficos e protocolos de autenticação. Convém que a força da identificação e autenticação de usuário seja adequada com a sensibilidade da informação a ser acessada.

Objetos como *tokens* de memória ou cartões inteligentes (*smart card*) que os usuários possuem também podem ser usados para identificação e autenticação. As tecnologias de autenticação biométrica que usam características ou atributos únicos de um indivíduo também podem ser usadas para autenticar a identidade de uma pessoa. Uma combinação de tecnologias e mecanismos seguramente relacionados resultará em uma autenticação forte.

11.5.3 Sistema de gerenciamento de senha

Controle
Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

Diretrizes para implementação
Convém que o sistema de gerenciamento de senha:

a) obrigue o uso de identificador de usuário (ID de usuário) e senha individual para manter responsabilidades;

b) permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

c) obrigue a escolha de senhas de qualidade (ver 11.3.1);

d) obrigue a troca de senhas (ver 11.3.1);

e) obrigue os usuários a trocar a senha temporária no primeiro acesso (ver 11.2.3);

f) mantenha um registro das senhas anteriores utilizadas e bloqueie a reutilização;

g) não mostre as senhas na tela quando forem digitadas;

h) armazene os arquivos de senha separadamente dos dados do sistema da aplicação;

i) armazene e transmita as senhas de forma protegida (por exemplo, criptografada ou *hashed*).

Informações adicionais
A senha é um dos principais meios de validar a autoridade de um usuário para acessar um serviço de computador.

Algumas aplicações requerem que senhas de usuário sejam atribuídas por uma autoridade independente. Em alguns casos, as alíneas b), d) e e) das diretrizes acima não se aplicam. Na maioria dos casos, as senhas são selecionadas e mantidas pelos usuários. Ver 11.3.1 para diretrizes do uso de senhas.

11.5.4 Uso de utilitários de sistema

Controle
Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado.

Diretrizes para implementação
Convém que as seguintes diretrizes para o uso de utilitários de sistema sejam consideradas:

a) uso de procedimentos de identificação, autenticação e autorização para utilitários de sistema;

b) segregação dos utilitários de sistema dos *softwares* de aplicação;

c) limitação do uso dos utilitários de sistema a um número mínimo de usuários confiáveis e autorizados (ver 11.2.2);

d) autorização para uso de utilitários de sistema não previstos;

e) limitação da disponibilidade dos utilitários de sistema, por exemplo para a duração de uma modificação autorizada;

f) registro de todo o uso de utilitários de sistemas;

g) definição e documentação dos níveis de autorização para os utilitários de sistema;

h) remoção ou desabilitação de todos os *softwares* utilitários e de sistema desnecessários;

i) não deixar utilitários de sistema disponíveis para usuários que têm acesso às aplicações nos sistemas onde segregação de funções é requerida.

Informações adicionais
A maioria das instalações de computadores tem um ou mais programas utilitários de sistema que podem ser capazes de sobrepor os controles dos sistemas e aplicações.

11.5.5 Limite de tempo de sessão

Controle
Convém que sessões inativas sejam encerradas após um período definido de inatividade.

Diretrizes para implementação
Convém que o recurso de limitação de tempo limpe a tela da sessão e também, possivelmente mais tarde, feche tanto a aplicação quanto as sessões de rede após um período definido de inatividade. Convém que o prazo de tempo para a desconexão reflita os riscos de segurança da área, a classificação da informação que está sendo manuseada, as aplicações que estão sendo utilizadas e os riscos relacionados para os usuários do terminal do equipamento.

Uma forma limitada para o recurso de limitação de tempo pode ser provida por alguns sistemas, os quais limpam a tela e previnem acesso não autorizado, mas não fecham as sessões das aplicações ou da rede.

Informações adicionais
Este controle é particularmente importante em locais de alto risco, os quais incluem áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização. Convém que estas sessões sejam encerradas para prevenir o acesso por pessoas não autorizadas e ataques de negação de serviço.

11.5.6 Limitação de horário de conexão

Controle
Convém que restrições nos horários de conexão sejam utilizadas para proporcionar segurança adicional para aplicações de alto risco.

Diretrizes para implementação
Convém que controles de horário de conexão sejam considerados para aplicações computacionais sensíveis, especialmente aquelas com terminais instalados em locais de alto risco, por exemplo em áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização. Exemplos deste tipo de restrição incluem:

a) utilização de janelas de tempo predeterminadas, por exemplo para transmissão de arquivos em lote ou sessões regulares interativas de curta duração;

b) restrição dos horários de conexão às horas normais de expediente se não houver necessidades para horas extras ou trabalhos fora do horário normal;

c) considerar a reautenticação em intervalos de tempo.

Informações adicionais
Limitar o período durante o qual as conexões de terminal para os serviços computadorizados são permitidas reduz a janela de oportunidade para acessos não autorizados. Limitar a duração de sessões ativas inibe os usuários a manter seções abertas, para evitar reautenticação.

11.6 Controle de acesso à aplicação e à informação

Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.

Convém que os recursos de segurança da informação sejam utilizados para restringir o acesso aos sistemas de aplicação.

Convém que o acesso lógico à aplicação e informação seja restrito a usuários autorizados. Convém que os sistemas de aplicação:

a) controlem o acesso dos usuários à informação e às funções dos sistemas de aplicação, de acordo com uma política de controle de acesso definida;

b) proporcionem proteção contra acesso não autorizado para qualquer *software* utilitário, sistema operacional e *software* malicioso que seja capaz de sobrepor ou contornar os controles da aplicação ou do sistema;

c) não comprometam outros sistemas com os quais os recursos de informação são compartilhados.

11.6.1 Restrição de acesso à informação

Controle
Convém que o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte seja restrito de acordo com o definido na política de controle de acesso.

Diretrizes para implementação
Convém que restrições para acesso sejam baseadas nos requisitos das aplicações individuais do negócio. Convém que a política de controle de acesso seja consistente com a política de acesso organizacional (ver 11.1).

Convém que a aplicação dos seguintes controles seja considerada de forma a suportar os requisitos de restrição de acesso:

a) fornecer menus para controlar o acesso às funções dos sistemas de aplicação;

b) controlar os direitos de acesso dos usuários, por exemplo, ler, escrever, excluir e executar;

c) controlar os direitos de acesso de outras aplicações;

d) assegurar que as saídas dos sistemas de aplicação que tratam informações sensíveis contenham apenas a informação relevante ao uso de tais saídas e são enviadas apenas para os terminais e locais autorizados; convém incluir uma análise crítica periódica de tais saídas, para assegurar que informação redundante seja removida.

11.6.2 Isolamento de sistemas sensíveis

Controle
Convém que sistemas sensíveis tenham um ambiente computacional dedicado (isolado).

Diretrizes para implementação
Convém que os seguintes pontos sejam considerados para o isolamento de um sistema sensível:

a) a sensibilidade de um sistema de aplicação seja explicitamente identificada e documentada pelo proprietário da aplicação (ver 7.1.2);

b) quando uma aplicação sensível é executada em um ambiente compartilhado, convém que se identifiquem os sistemas de aplicação com os quais ela compartilhará recursos e os correspondentes riscos, e que se obtenha a concordância do proprietário da aplicação sensível.

Informações adicionais
Alguns sistemas de aplicação são suficientemente sensíveis a perdas potenciais, requerendo tratamento especial. A sensibilidade pode indicar que o sistema de aplicação:

a) seja executado a partir de um computador dedicado; ou

b) compartilha recursos somente com sistemas de aplicação confiáveis.

O isolamento pode ser obtido utilizando-se métodos físicos ou lógicos (ver 11.4.5).

11.7 Computação móvel e trabalho remoto

Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

Convém que a proteção requerida seja proporcional com o risco desta forma específica de trabalho. Quando se utiliza a computação móvel, convém que os riscos de trabalhar em um ambiente desprotegido sejam considerados e a proteção adequada seja aplicada. No caso de trabalho remoto, convém que a organização aplique proteção ao local do trabalho remoto e assegure que as providências adequadas estão implementadas para este tipo de trabalho.

11.7.1 Computação e comunicação móvel

Controle
Convém que uma política formal seja estabelecida e que medidas de segurança apropriadas sejam adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.

Diretrizes para implementação
Quando se utilizam recursos de computação e comunicação móveis, como, por exemplo, *notebooks*, *palmtops*, *laptops*, cartões inteligentes (*smart cards*) e telefones celulares, convém que cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas. A política de computação móvel deve levar em consideração os riscos de se trabalhar com equipamentos de computação móvel em ambientes desprotegidos.

Convém que a política de computação móvel inclua os requisitos de proteção física, controles de acesso, técnicas criptográficas, cópias de segurança e proteção contra vírus. Convém que esta política inclua também regras e recomendações sobre a conexão de recursos móveis à rede e diretrizes sobre o uso destes recursos em locais públicos.

Convém que sejam tomadas certas precauções ao se utilizarem os recursos de computação móvel em locais públicos, salas de reuniões e outras áreas desprotegidas fora dos limites da organização. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nestes recursos, por exemplo através da utilização de técnicas de criptografia (ver 12.3).

Convém que usuários de recursos de computação móvel em locais públicos tomem cuidado para evitar o risco de captação por pessoas não autorizadas. Convém que procedimentos contra *softwares* maliciosos sejam estabelecidos e mantidos sempre atualizados (ver 10.4).

Convém que cópias de segurança das informações críticas de negócio sejam feitas regularmente. Convém que equipamentos estejam disponíveis para possibilitar a realização de cópias de segurança das informações de forma rápida e fácil. Para essas cópias de segurança, convém que sejam adotadas proteções adequadas contra, por exemplo, furto ou roubo, ou perda de informação.

Convém que proteção adequada seja dada para o uso dos recursos de computação móvel conectados em rede. Convém que o acesso remoto às informações do negócio através de redes públicas, usando os recursos de computação móvel, ocorra apenas após o sucesso da identificação e da autenticação, e com os apropriados mecanismos de controle de acesso implantados (ver 11.4).

Convém que os recursos de computação móvel também estejam protegidos fisicamente contra furto ou roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião. Convém que esteja estabelecido um procedimento específico que leve em consideração requisitos legais, securitários e outros requisitos de segurança da organização para casos de roubo ou perda de recursos de computação móvel. Convém que os equipamentos que contêm informações importantes, sensíveis e/ou críticas para o negócio não sejam deixados sem observação e, quando possível, estejam fisicamente trancados, ou convém que travas especiais sejam utilizadas para proteger o equipamento. (ver 9.2.5).

Convém que seja providenciado treinamento para os usuários de computação móvel, para aumentar o nível de conscientização a respeito dos riscos adicionais resultantes desta forma de trabalho e dos controles que devem ser implementados.

Informações adicionais
As redes de conexão sem fio são similares a outros tipos de redes, mas possuem diferenças importantes que convém que sejam consideradas quando da identificação de controles. As diferenças típicas são:

a) alguns protocolos de segurança de redes sem fio são imaturos e possuem fragilidades conhecidas;

b) pode não ser possível efetuar cópias de segurança das informações armazenadas em computadores móveis devido à largura de banda limitada e/ou devido ao equipamento móvel não estar conectado no momento em que as cópias de segurança estão programadas.

11.7.2 Trabalho remoto

Controle
Convém que uma política, planos operacionais e procedimentos sejam desenvolvidos e implementados para atividades de trabalho remoto.

Diretrizes para implementação
Convém que as organizações somente autorizem atividades de trabalho remotas apenas se elas estiverem certas de que as providências apropriadas e controles de segurança estão implementados e que estes estão de acordo com a política de segurança da organização.

Convém que a proteção apropriada ao local do trabalho remoto seja implantada para evitar, por exemplo, o furto ou roubo do equipamento e de informações, a divulgação não autorizada de informação, o acesso remoto não autorizado aos sistemas internos da organização ou mau uso de recursos. Convém que o trabalho remoto seja autorizado e controlado pelo gestor e convém que sejam asseguradas as providências adequadas a esta forma de trabalho.

Convém que os seguintes pontos sejam considerados:

a) a segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;

b) o ambiente físico proposto para o trabalho remoto;

c) os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;

d) a ameaça de acesso não autorizado à informação ou aos recursos por outras pessoas que utilizam o local, por exemplo familiares e amigos;

e) o uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;

f) políticas e procedimentos para evitar disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

g) acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), que pode ser proibido legalmente;

h) acordos de licenciamento de *software* que podem tornar as organizações responsáveis pelo licenciamento do *software* cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros;

i) requisitos de proteção contra vírus e requisitos de *firewall*.

Convém que as diretrizes e providências a serem consideradas incluam:

a) a provisão de equipamento e mobília apropriados às atividade de trabalho remoto, onde o uso de equipamentos de propriedade particular que não esteja sob controle da organização não é permitido;

b) uma definição do trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;

c) a provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;

d) segurança física;

e) regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;

f) a provisão de suporte e manutenção de *hardware* e *software*;

g) a provisão de seguro;

h) os procedimentos para cópias de segurança e continuidade do negócio;

i) auditoria e monitoramento da segurança;

j) revogação de autoridade e direitos de acesso, e devolução do equipamento quando as atividades de trabalho remoto cessarem.

<u>Informações adicionais</u>
As atividades de trabalho remoto utilizam tecnologias de comunicação que permitem que as pessoas trabalhem remotamente de uma localidade fixa externa à sua organização.

12 Aquisição, desenvolvimento e manutenção de sistemas de informação

12.1 Requisitos de segurança de sistemas de informação

Objetivo: Garantir que segurança é parte integrante de sistemas de informação.

Sistemas de informação incluem sistemas operacionais, infra-estrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário. O projeto e a implementação de sistemas de informação destinados a apoiar o processo de negócios podem ser cruciais para a segurança. Convém que os requisitos de segurança sejam identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação.

Convém que todos os requisitos de segurança sejam identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios para um sistema de informações.

12.1.1 Análise e especificação dos requisitos de segurança

Controle
Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.

Diretrizes para implementação
Convém que as especificações para os requisitos de controles, nos sistemas de informação, considerem os controles automáticos a serem incorporados, assim como a necessidade de apoiar controles manuais. Convém que considerações similares sejam aplicadas quando da avaliação de pacotes de *softwares*, desenvolvidos internamente ou comprados, para as aplicações de negócios.

Convém que requisitos de segurança e controles reflitam o valor para o negócio dos ativos de informação envolvidos (ver 7.2), e os danos potenciais ao negócio que poderiam resultar de uma falha ou ausência de segurança.

Convém que os requisitos de sistemas para a segurança da informação, bem como os processos para implementá-la sejam integrados aos estágios iniciais dos projetos dos sistemas de informação. Controles introduzidos no estágio de projeto são significativamente mais baratos para implementar e manter do que aqueles incluídos durante ou após a implementação.

Convém que, no caso de produtos comprados, um processo formal de aquisição e testes seja seguido. Convém que contratos com fornecedores levem em consideração os requisitos de segurança identificados. Nas situações em que funcionalidades de segurança de um produto proposto não satisfaçam requisitos especificados, convém que o risco introduzido, assim como os controles associados, sejam reconsiderados antes da compra do produto. Nas situações em que as funcionalidades adicionais incorporadas acarretem riscos à segurança, convém que estas sejam desativadas ou a estrutura de controles proposta seja analisada criticamente para determinar se há vantagem na utilização das funcionalidades em questão.

Informações adicionais
Se considerado apropriado, por exemplo, por razões de custos, o gestor pode considerar o uso de produtos avaliados e certificados por entidade independente. Informação adicional sobre critérios de avaliação de produtos pode ser encontrada na ISO/IEC 15408 ou em outras normas de avaliação ou certificação apropriadas.

A ISO/IEC 13335-3 possui orientação sobre o uso de processos de gerenciamento de riscos para a identificação de requisitos de controles de segurança.

12.2 Processamento correto nas aplicações

Objetivo: Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

Convém que controles apropriados sejam incorporados no projeto das aplicações, inclusive aquelas desenvolvidas pelos usuários, para assegurar o processamento correto. Convém que esses controles incluam a validação dos dados de entrada, do processamento interno e dos dados de saída.

Controles adicionais podem ser necessários para sistemas que processem informações sensíveis, valiosas ou críticas, ou que nestas exerçam algum impacto. Convém que tais controles sejam determinados com base em requisitos de segurança e a análise/avaliação de riscos.

12.2.1 Validação dos dados de entrada

Controle
Convém que os dados de entrada de aplicações sejam validados para garantir que são corretos e apropriados.

Diretrizes para implementação
Convém que sejam aplicadas checagens na entrada de transações de negócios, em dados permanentes (por exemplo, nomes e endereços, limites de crédito, números de referência de clientes) e em, parâmetros de tabelas (por exemplo, preços de venda, taxas de conversão de moedas, tarifas de impostos). Convém que as seguintes diretrizes sejam consideradas:

a) entrada duplicada ou outros tipos de verificação, tais como checagem de limites ou campos limitando as faixas específicas de dados de entrada, para detectar os seguintes erros:

   1) valores fora de faixa;

   2) caracteres inválidos em campos de dados;

   3) dados incompletos ou faltantes;

   4) volumes de dados excedendo limites superiores ou inferiores;

   5) dados de controle inconsistentes ou não autorizados;

b) verificação periódica do conteúdo de campos-chave ou arquivos de dados para confirmar a sua validade e integridade;

c) inspeção de cópias impressas de documentos de entrada para detectar quaisquer alterações não autorizadas (convém que todas as mudanças em documentos de entrada sejam autorizadas);

d) procedimentos para tratar erros de validação;

e) procedimentos para testar a plausibilidade dos dados de entrada;

f) definição da responsabilidade de todo o pessoal envolvido no processo de entrada de dados;

g) criação de um registro de atividades envolvendo o processo de entrada de dados (ver 10.10.1).

Informações adicionais
A verificação e validação automática de dados de entrada podem ser consideradas, onde aplicáveis, para reduzir o risco de erros e prevenir ataques conhecidos como *buffer overflow* e injeção de código.

12.2.2 Controle do processamento interno

Controle
Convém que sejam incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.

Diretrizes para implementação
Convém que o projeto e a implementação das aplicações garantam que os riscos de falhas de processamento que levem à perda de integridade sejam minimizados. Áreas específicas a serem consideradas incluem:

a) o uso das funções, como incluir, modificar e remover para implementação de alterações nos dados;

b) procedimentos para evitar que programas rodem na ordem errada ou continuem rodando após uma falha de processamento (ver 10.1.1);

c) o uso de programas apropriados para recuperação de falhas, para assegurar o processamento correto dos dados;

d) proteção contra ataques usando *buffer overrun/overflow*;

Convém que seja preparada uma lista de verificação apropriada, as atividades sejam documentadas e os resultados sejam mantidos em segurança. Exemplos de verificações que podem ser incorporadas incluem:

a) controles de sessões ou de lotes, para reconciliar saldos de arquivos após as atualizações de transações;

b) controles de saldos, para verificação de saldos abertos comparando com saldos previamente encerrados o batimento de saldos de abertura contra saldos de fechamento, utilizando:

   1) controles *run-to-run*;

   2) totalizações na atualização de arquivos;

   3) controles *program-to-program*;

c) validação de dados de entrada gerados pelo sistema (ver 12.2.1);

d) verificações de integridade, autenticidade ou qualquer outra característica de segurança, de dados ou *softwares* transferidos, ou atualizados entre computadores centrais e remotos;

e) implementação de técnicas de consistência (*hash*) para registros e arquivos;

f) verificações para garantir que os programas sejam rodados no tempo correto;

g) verificações para garantir que os programas sejam rodados na ordem correta e terminem em caso de falha, e que qualquer processamento adicional seja estancado, até que o problema seja resolvido;

h) criação de um registro das atividades envolvidas no processamento (ver 10.10.1).

Informações adicionais
Os dados que tenham sido corretamente alimentados podem ser corrompidos por falhas de *hardware*, erros de processamento ou por atos deliberados. As verificações de validação requeridas dependem da natureza das aplicações e do impacto, no negócio, de qualquer corrupção de dados.

12.2.3 Integridade de mensagens

Controle
Convém que requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações sejam identificados e os controles apropriados sejam identificados e implementados.

Diretrizes para implementação
Convém que seja efetuada uma análise/avaliação dos riscos de segurança para determinar se a integridade das mensagens é requerida e para identificar o método mais apropriado de implementação.

Informações adicionais
As técnicas criptográficas (ver 12.3) podem ser usadas como um meio apropriado para a implementação da autenticação de mensagens.

12.2.4 Validação de dados de saída

Controle
Convém que os dados de saída das aplicações sejam validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

Diretrizes para implementação
A validação de dados de saída pode incluir:

a) verificações de plausibilidade para testar se os dados de saída são razoáveis;

b) controles envolvendo contagens de reconciliação para garantir o processamento de todos os dados;

c) fornecimento de informação suficiente para que um leitor ou um sistema de processamento subseqüente possa determinar a exatidão, completeza, precisão e classificação das informações;

d) procedimentos para responder aos testes de validação dos dados de saída;

e) definição das responsabilidades de todo o pessoal envolvido no processo de dados de saída;

f) criação de um registro de atividades do processo de validação dos dados de saída.

Informações adicionais
Tipicamente, sistemas e aplicações são construídos no pressuposto de que, tendo sido efetuadas as validações apropriadas, verificações e testes, as saídas estarão sempre corretas. Contudo, este pressuposto nem sempre é válido, isto é, sistemas que tenham sido testados podem ainda produzir dados de saída incorretos sob certas circunstâncias.

12.3 Controles criptográficos

Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Convém que uma política seja desenvolvida para o uso de controles criptográficos. Convém que o gerenciamento de chaves seja implementado para apoiar o uso de técnicas criptográficas.

12.3.1 Política para o uso de controles criptográficos

Controle
Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.

Diretrizes para implementação
Convém que, quando do desenvolvimento de uma política para criptografia, sejam considerados:

a) a abordagem gerencial quanto ao uso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações de negócio sejam protegidas (ver 5.1.1);

b) a identificação do nível requerido de proteção com base em uma análise/avaliação de riscos, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido;

c) o uso de criptografia para a proteção de informações sensíveis transportadas em celulares e PDA, mídias removíveis ou móveis, dispositivos ou linhas de comunicação;

d) a abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas;

e) papéis e responsabilidades, por exemplo, de quem for responsável:

   1) pela implementação da política;

   2) pelo gerenciamento de chaves, incluindo sua geração (ver 12.3.2);

f) os padrões a serem adotados para a efetiva implementação ao longo de toda a organização (qual solução é usada para quais processos de negócios);

g) o impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdos (por exemplo, detecção de vírus).

Convém que sejam consideradas, na implementação da política criptográfica da organização, as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e das questões relativas ao fluxo transfronteiras de informações cifradas (ver 15.1.6).

Controles criptográficos podem ser usados para alcançar diversos objetivos de segurança, como, por exemplo:

a) confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

b) integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para proteger a autenticidade e integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;

c) não-repúdio: usando técnicas de criptografia para obter prova da ocorrência ou não ocorrência de um evento ou ação.

Informações adicionais
Convém que a tomada de decisão para verificar se uma solução de criptografia é apropriada seja vista como parte de um processo de análise/avaliação de riscos e seleção de controles mais amplos. Essa avaliação pode, então, ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle seja usado e para que propósito e processos de negócios.

Uma política sobre o uso de controles criptográficos é necessária para maximizar os benefícios e minimizar os riscos do uso de técnicas criptográficas para evitar o uso incorreto ou inapropriado. Quanto ao uso de assinaturas digitais, convém que seja considerada toda a legislação relevante, em particular aquela que descreve as condições sob as quais uma assinatura digital é legalmente aceita (ver 15.1).

Convém que seja buscada a opinião de um especialista para identificar o nível apropriado de proteção e definir as especificações aplicáveis que proporcionarão o nível requerido de proteção e o apoio à implementação de um sistema seguro de gerenciamento de chaves (ver 12.3.2).

O ISO/IEC JTC1 SC27 desenvolveu diversas normas relacionadas com controles criptográficos. Informações adicionais podem também ser encontradas na IEEE P1363 e no *OECD Guidelines on Cryptography*.

12.3.2 Gerenciamento de chaves

Controle
Convém que um processo de gerenciamento de chaves seja implantado para apoiar o uso de técnicas criptográficas pela organização.

Diretrizes para implementação
Convém que todas as chaves criptográficas sejam protegidas contra modificação, perda e destruição. Adicionalmente, chaves secretas e privadas necessitam de proteção contra a divulgação não autorizada. Convém que os equipamentos utilizados para gerar, armazenar e guardar as chaves sejam fisicamente protegidos.

Convém que um sistema de gerenciamento de chaves seja baseado em um conjunto estabelecido de normas, procedimentos e métodos de segurança para:

a) gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;

b) gerar e obter certificados de chaves públicas;

c) distribuir chaves para os usuários devidos, incluindo a forma como as chaves devem ser ativadas, quando recebidas;

d) armazenar chaves, incluindo a forma como os usuários autorizados obtêm acesso a elas;

e) mudar ou atualizar chaves, incluindo regras relativas a quando as chaves devem ser mudadas e como isto será feito;

f) lidar com chaves comprometidas;

g) revogar chaves, incluindo regras de como elas devem ser retiradas ou desativadas, por exemplo quando chaves tiverem sido comprometidas ou quando um usuário deixa a organização (convém que, também neste caso, que as chaves sejam guardadas);

h) recuperar chaves perdidas ou corrompidas, como parte da gestão da continuidade do negócio, por exemplo para recuperação de informações cifradas;

i) guardar chaves, por exemplo para informações guardadas ou armazenadas em cópias de segurança;

j) destruir chaves;

k) manter registro e auditoria das atividades relacionadas com o gerenciamento de chaves.

Convém, para reduzir a possibilidade de comprometimento, que datas de ativação e desativação de chaves sejam definidas de forma que possam ser utilizadas apenas por um período de tempo limitado. Convém que este período de tempo seja dependente das circunstâncias sob as quais o controle criptográfico está sendo usado, assim como do risco percebido.

Além do gerenciamento seguro de chaves secretas e privadas, convém que a autenticidade de chaves públicas seja também considerada. Este processo de autenticação pode ser conduzido utilizando-se certificados de chaves públicas que são normalmente emitidos por uma autoridade certificadora, a qual convém que seja uma organização reconhecida, com controles adequados e procedimentos implantados com o objetivo de garantir o requerido nível de confiança.

Convém que o conteúdo dos termos dos acordos de nível de serviço ou contratos com fornecedores externos de serviços criptográficos, por exemplo com uma autoridade certificadora, cubram aspectos como responsabilidades, confiabilidade dos serviços e tempos de resposta para a execução dos serviços contratados (ver 6.2.3).

Informações adicionais
O gerenciamento de chaves criptográficas é essencial para o uso efetivo de técnicas criptográficas. A ISO/IEC 11770 fornece informação adicional sobre gerenciamento de chaves. Os dois tipos de técnicas criptográficas são:

a) técnicas de chaves secretas, onde duas ou mais partes compartilham a mesma chave, a qual é utilizado tanto para cifrar quanto para decifrar a informação; esta chave deve ser mantida secreta, uma vez que qualquer um que tenha acesso a ela será capaz de decifrar todas as informações que tenham sido cifradas com essa chave ou dela se utilizando para introduzir informação não autorizada;

b) técnicas de chaves públicas, onde cada usuário possui um par de chaves; uma chave pública (que pode ser revelada para qualquer um) e uma chave privada (que deve ser mantida secreta); técnicas de chaves públicas podem ser utilizadas para cifrar e para produzir assinaturas digitais (ver também ISO/IEC 9796 e ISO/IEC 14888).

Existe a ameaça de que seja forjada uma assinatura digital pela substituição da chave pública do usuário. Este problema é resolvido pelo uso de um certificado de chave pública.

Técnicas criptográficas podem ser também utilizadas para proteger chaves criptográficas. Pode ser necessário o estabelecimento de procedimentos para a manipulação de solicitações legais para acesso a chaves criptográficas, por exemplo, informação cifrada pode ser requerida em sua forma decifrada para uso como evidência em um processo judicial.

12.4 Segurança dos arquivos do sistema

Objetivo: Garantir a segurança de arquivos de sistema.

Convém que o acesso aos arquivos de sistema e aos programas de código fonte seja controlado e que atividades de projeto de tecnologia da informação e de suporte sejam conduzidas de forma segura. Convém que cuidados sejam tomados para evitar a exposição de dados sensíveis em ambientes de teste.

12.4.1 Controle de *software* operacional

Controle
Convém que procedimentos para controlar a instalação de *software* em sistemas operacionais sejam implementados.

Diretrizes para implementação
Para minimizar o risco de corrupção aos sistemas operacionais, convém que as seguintes diretrizes sejam consideradas para controlar mudanças:

a) a atualização do *software* operacional, de aplicativos e de bibliotecas de programas seja executada somente por administradores treinados e com autorização gerencial (ver 12.4.3);

b) sistemas operacionais somente contenham código executável e aprovado, e não contenham códigos em desenvolvimento ou compiladores;

c) sistemas operacionais e aplicativos somente sejam implementados após testes extensivos e bem-sucedidos; é recomendável que os testes incluam testes sobre uso, segurança, efeitos sobre outros sistemas, como também sobre uso amigável, e sejam realizados em sistemas separados (ver 10.1.4); convém que seja assegurado que todas as bibliotecas de programa-fonte correspondentes tenham sido atualizadas;

d) um sistema de controle de configuração seja utilizado para manter controle da implementação do *software* assim como da documentação do sistema;

e) uma estratégia de retorno às condições anteriores seja disponibilizada antes que mudanças sejam implementadas no sistema;

f) um registro de auditoria seja mantido para todas as atualizações das bibliotecas dos programas operacionais;

g) versões anteriores dos *softwares* aplicativos sejam mantidas como medida de contingência;

h) versões antigas de *software* sejam arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações e *software* de suporte durante um prazo igual ao prazo de retenção dos dados.

Convém que *software* adquirido de fornecedores e utilizado em sistemas operacionais seja mantido num nível apoiado pelo fornecedor. Ao transcorrer do tempo, fornecedores de *software* cessam o apoio às versões antigas do *software*. Convém que a organização considere os riscos associados à dependência de *software* sem suporte.

Convém que qualquer decisão de atualização para uma nova versão considere os requisitos do negócio para a mudança e da segurança associada, por exemplo, a introdução de uma nova funcionalidade de segurança ou a quantidade e a gravidade dos problemas de segurança associados a esta versão. Convém que pacotes de correções de *software* sejam aplicados quando puderem remover ou reduzir as vulnerabilidades de segurança (ver 12.6.1).

Convém que acessos físicos e lógicos sejam concedidos a fornecedores, quando necessário, para a finalidade de suporte e com aprovação gerencial. Convém que as atividades do fornecedor sejam monitoradas.

Os *softwares* para computadores podem depender de outros *softwares* e módulos fornecidos externamente, os quais convém ser monitorados e controlados para evitar mudanças não autorizadas, que podem introduzir fragilidades na segurança.

Informações adicionais
Convém que sistemas operacionais sejam atualizados quando existir um requisito para tal, por exemplo, se a versão atual do sistema operacional não suportar mais os requisitos do negócio. Convém que as atualizações não sejam efetivadas pela mera disponibilidade de uma versão nova do sistema operacional. Novas versões de sistemas operacionais podem ser menos seguras, com menor estabilidade, e ser menos entendidas do que os sistemas atuais.

12.4.2 Proteção dos dados para teste de sistema

Controle
Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

Diretrizes para implementação
Para propósitos de teste, convém que seja evitado o uso de bancos de dados operacionais que contenham informações de natureza pessoal ou qualquer outra informação considerada sensível. Se informação de natureza pessoal ou outras informações sensíveis forem utilizadas com o propósito de teste, convém que todos os detalhes e conteúdo sensível sejam removidos ou modificados de forma a evitar reconhecimento antes do seu uso. Convém que sejam aplicadas as seguintes diretrizes para a proteção de dados operacionais, quando utilizados para fins de teste:

a) os procedimentos de controle de acesso, aplicáveis aos aplicativos de sistema em ambiente operacional, sejam também aplicados aos aplicativos de sistema em ambiente de teste;

b) seja obtida autorização cada vez que for utilizada uma cópia da informação operacional para uso de um aplicativo em teste;

c) a informação operacional seja apagada do aplicativo em teste imediatamente após completar o teste;

d) a cópia e o uso de informação operacional sejam registrados de forma a prover uma trilha para auditoria.

Informações adicionais
Testes de sistema e testes de aceitação requerem normalmente volumes significativos de dados de teste que sejam o mais próximo possível aos dados utilizados no ambiente operacional.

12.4.3 Controle de acesso ao código-fonte de programa

Controle
Convém que o acesso ao código-fonte de programa seja restrito.

Diretrizes para implementação
Convém que o acesso ao código-fonte de programa e de itens associados (como desenhos, especificações, planos de verificação e de validação) seja estritamente controlado, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais. Para os códigos-fonte de programas, este controle pode ser obtido com a guarda centralizada do código, de preferência utilizando bibliotecas de programa-fonte. Convém que as seguintes orientações sejam consideradas (ver seção 11) para o controle de acesso às bibliotecas de programa-fonte, com a finalidade de reduzir o risco de corrupção de programas de computador:

a) quando possível, seja evitado manter as bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais;

b) seja implementado o controle do código-fonte de programa e das bibliotecas de programa-fonte, conforme procedimentos estabelecidos;

c) o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte;

d) a atualização das bibliotecas de programa-fonte e itens associados e a entrega de fontes de programas a programadores seja apenas efetuada após o recebimento da autorização pertinente;

e) as listagens dos programas sejam mantidas num ambiente seguro (ver 10.7.4);

f) seja mantido um registro de auditoria de todos os acessos a código-fonte de programa;

g) a manutenção e a cópia das bibliotecas de programa-fonte estejam sujeitas a procedimentos estritos de controles de mudanças (ver 12.5.1);

Informações adicionais
Os códigos-fonte de programas são códigos escritos por programadores, que são compilados (e ligados) para criar programas executáveis. Algumas linguagens de programação não fazem uma distinção formal entre código-fonte e executável, pois os executáveis são criados no momento da sua ativação.

As ABNT NBR ISO 10007 e ABNT NBR ISO/IEC 12207 possuem mais informações sobre a gestão de configuração e o processo de ciclo de vida de *software*.

12.5 Segurança em processos de desenvolvimento e de suporte

Objetivo: Manter a segurança de sistemas aplicativos e da informação.

Convém que os ambientes de projeto e de suporte sejam estritamente controlados.

Convém que os gerentes responsáveis pelos sistemas aplicativos sejam também responsáveis pela segurança dos ambientes de projeto ou de suporte. Convém que eles assegurem que mudanças propostas sejam analisadas criticamente para verificar que não comprometam a segurança do sistema ou do ambiente operacional.

12.5.1 Procedimentos para controle de mudanças

Controle
Convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças.

Diretrizes para implementação
Convém que os procedimentos de controle de mudanças sejam documentados e reforçados com a finalidade de minimizar a corrupção dos sistemas da informação. Convém que a introdução de novos sistemas e mudanças maiores em sistemas existentes sigam um processo formal de documentação, especificação, teste, controle da qualidade e gestão da implementação.

Convém que o processo inclua uma análise/avaliação de riscos, análise do impacto das mudanças e a especificação dos controles de segurança requeridos. Convém que o processo garanta que a segurança e os procedimentos de controle atuais não sejam comprometidos, que os programadores de suporte tenham acesso somente às partes do sistema necessárias para o cumprimento das tarefas e que sejam obtidas concordância e aprovação formal para qualquer mudança obtida.

Convém que, quando praticável, os procedimentos de controle de mudanças sejam integrados (ver 10.1.2). Convém que os procedimentos de mudanças incluam:

a) a manutenção de um registro dos níveis acordados de autorização;

b) a garantia de que as mudanças sejam submetidas por usuários autorizados;

c) a análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

d) a identificação de todo *software*, informação, entidades em bancos de dados e *hardware* que precisam de emendas;

e) a obtenção de aprovação formal para propostas detalhadas antes da implementação;

f) a garantia da aceitação das mudanças por usuários autorizados, antes da implementação;

g) a garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada ou descartada;

h) a manutenção de um controle de versão de todas as atualizações de *softwares*;

i) a manutenção de uma trilha para auditoria de todas as mudanças solicitadas;

j) a garantia de que toda a documentação operacional (ver 10.1.1) e procedimentos dos usuários sejam alterados conforme necessário e que se mantenham apropriados;

k) a garantia de que as mudanças sejam implementadas em horários apropriados, sem a perturbação dos processos de negócios cabíveis.

Informações adicionais
A mudança de *software* pode ter impacto no ambiente operacional.

As boas práticas incluem o teste de novos *softwares* em um ambiente segregado dos ambientes de produção e de desenvolvimento (ver 10.1.4). Isto fornece um meio de controle sobre o novo *software* e permite uma proteção adicional à informação operacional que é utilizada para propósitos de teste. Aplica-se também às correções, pacotes de serviço e outras atualizações. Convém que atualizações automáticas não sejam utilizadas em sistemas críticos, pois algumas atualizações podem causar falhas em aplicações críticas (ver 12.6).

12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional

Controle
Convém que aplicações críticas de negócios sejam analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.

Diretrizes para implementação
Convém que o processo compreenda:

a) uma análise crítica dos procedimentos de controle e integridade dos controles para assegurar que não foram comprometidos pelas mudanças no sistema operacional;

b) a garantia de que o plano anual de suporte e o orçamento irão cobrir as análises e testes do sistema devido às mudanças no sistema operacional;

c) a garantia de que as mudanças pretendidas sejam comunicadas em tempo hábil para permitir os testes e análises críticas antes da implementação das mudanças;

d) a garantia de que as mudanças necessárias sejam executadas nos planos de continuidade de negócios (ver seção 14).

Convém que seja dada responsabilidade a um grupo específico ou a um indivíduo para monitoramento das vulnerabilidades e divulgação de emendas e correções dos fornecedores de *software* (ver 12.6).

12.5.3 Restrições sobre mudanças em pacotes de *software*

Controle
Convém que modificações em pacotes de *software* sejam desencorajadas e limitadas às mudanças necessárias e que todas as mudanças sejam estritamente controladas.

Diretrizes para implementação
Quando possível e praticável, convém que pacotes de *softwares* providos pelos fornecedores sejam utilizados sem modificações. Quando um pacote de *software* requer modificação, convém que sejam considerados os seguintes itens:

a) o risco de que controles e processos de integridade embutidos no *software* sejam comprometidos;

b) a obtenção do consentimento do fornecedor;

c) a possibilidade de obtenção junto ao fornecedor das mudanças necessárias como atualização padrão do programa;

d) o impacto resultante quando a organização passa a ser responsável para a manutenção futura do *software* como resultado das mudanças.

Se mudanças forem necessárias, convém que o *software* original seja mantido e as mudanças aplicadas numa cópia claramente identificada. Convém que um processo de gestão de atualizações seja implementado para assegurar a instalação das mais recentes correções e atualizações para todos os *softwares* autorizados (ver 12.6). Convém que todas as mudanças sejam completamente testadas e documentadas para que possam ser reaplicadas, se necessário, em atualizações futuras do *software*. Se requerido, convém que as modificações sejam testadas e validadas por um grupo de avaliação independente.

12.5.4 Vazamento de informações

Controle
Convém que oportunidades para vazamento de informações sejam prevenidas.

Diretrizes para implementação
Convém que os seguintes itens sejam considerados, para limitar o risco de vazamento de informações, por exemplo através do uso e exploração de *covert channels*:

a) a varredura do envio de mídia e comunicações para verificar a presença de informação oculta;

b) o mascaramento e a modulação do comportamento dos sistemas e das comunicações para reduzir a possibilidade de terceiros deduzirem informações a partir do comportamento dos sistemas;

c) a utilização de sistemas e *software* reconhecidos como de alta integridade, por exemplo utilizando produtos avaliados (ver ISO/IEC 15408);

d) o monitoramento regular das atividades do pessoal e do sistema, quando permitido pela legislação ou regulamentação vigente;

e) o monitoramento do uso de recursos de sistemas de computação.

Informações adicionais
Os *covert channels* são caminhos não previstos para conduzir fluxo de informações, mas que no entanto podem existir num sistema ou rede. Por exemplo, a manipulação de *bits* no protocolo de pacotes de comunicação poderia ser utilizada como um método oculto de sinalização. Devido à sua natureza, seria difícil, se não impossível, precaver-se contra a existência de todos os possíveis *covert channels*. No entanto, a exploração destes canais freqüentemente é realizada por código troiano (ver 10.4.1). A adoção de medidas de proteção contra código troiano reduz, conseqüentemente, o risco de exploração de *covert channels*.

A precaução contra acesso não autorizado à rede (ver 11.4), como também políticas e procedimentos para dissuadir o mau uso de serviços de informação pelo pessoal (ver 15.1.5), pode ajudar a proteger contra *covert channels*.

12.5.5 Desenvolvimento terceirizado de *software*

Controle
Convém que a organização supervisione e monitore o desenvolvimento terceirizado de *software*.

Diretrizes para implementação
Convém que sejam considerados os seguintes itens quando do desenvolvimento de *software* terceirizado:

a) acordos de licenciamento, propriedade do código e direitos de propriedade intelectual (ver 15.1.2);

b) certificação da qualidade e exatidão do serviço realizado;

c) provisões para custódia no caso de falha da terceira parte;

d) direitos de acesso para auditorias de qualidade e exatidão do serviço realizado;

e) requisitos contratuais para a qualidade e funcionalidade da segurança do código;

f) testes antes da instalação para detectar a presença de código malicioso e troiano.

12.6 Gestão de vulnerabilidades técnicas

Objetivo: Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas. Convém que a implementação da gestão de vulnerabilidades técnicas seja implementada de forma efetiva, sistemática e de forma repetível com medições de confirmação da efetividade. Convém que estas considerações incluam sistemas operacionais e quaisquer outras aplicações em uso.

12.6.1 Controle de vulnerabilidades técnicas

Controle
Convém que seja obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.

Diretrizes para implementação
Um inventário completo e atualizado dos ativos de informação (ver 7.1) é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica. Informação específica para o apoio à gestão de vulnerabilidade técnica inclui o fornecedor de *software*, o número de versão, o *status* atual de uso e distribuição (por exemplo, que *softwares* estão instalados e em quais sistemas) e a(s) pessoa(s) na organização responsável(is) pelos *softwares*.

Convém que a ação apropriada seja tomada, no devido tempo, como resposta às potenciais vulnerabilidades técnicas identificadas. Convém que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas:

a) a organização defina e estabeleça as funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a análise/avaliação de riscos de vulnerabilidades, *patches*, acompanhamento dos ativos e qualquer coordenação de responsabilidades requerida;

b) os recursos de informação a serem usados para a identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre eles sejam identificados para *softwares* e outras tecnologias (com base na lista de inventário dos ativos, ver 7.1.1); convém que esses recursos de informação sejam mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis forem encontrados;

c) seja definido um prazo para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;

d) uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização avalie os riscos associados e as ações a serem tomadas; tais ações podem requerer o uso de *patches* nos sistemas vulneráveis e/ou a aplicação de outros controles;

e) dependendo da urgência exigida para tratar uma vulnerabilidade técnica, convém que a ação tomada esteja de acordo com os controles relacionados com a gestão de mudanças (ver 12.5.1) ou que sejam seguidos os procedimentos de resposta a incidentes de segurança da informação (ver 13.2);

f) se um *patch* for disponibilizado, convém que sejam avaliados os riscos associados à sua instalação (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação do *patch*);

g) *patches* sejam testados e avaliados antes de serem instaladas para assegurar a efetividade e que não tragam efeitos que não possam ser tolerados; quando não existir a disponibilidade de um *patch*, convém considerar o uso de outros controles, tais como:

   1) a desativação de serviços ou potencialidades relacionadas à vulnerabilidade;

   2) a adaptação ou agregação de controles de acesso, por exemplo *firewalls* nas fronteiras da rede (ver 11.4.5);

   3) o aumento do monitoramento para detectar ou prevenir ataques reais;

   4) o aumento da conscientização sobre a vulnerabilidade;

h) seja mantido um registro de auditoria de todos os procedimentos realizados;

i) com a finalidade de assegurar a eficácia e a eficiência, convém que seja monitorado e avaliado regularmente o processo de gestão de vulnerabilidades técnicas;

j) convém abordar em primeiro lugar os sistemas com altos riscos.

<u>Informações adicionais</u>
O correto funcionamento do processo de gestão de vulnerabilidades técnicas é crítico para muitas organizações e, portanto, convém que seja monitorado regularmente. Um inventário de ativos preciso é essencial para assegurar que vulnerabilidades potenciais relevantes sejam identificadas.

A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças e, como tal, pode aproveitar os procedimentos e processos da gestão de mudanças (ver 10.1.2 e 12.5.1).

Os fornecedores estão sempre sob grande pressão para liberar *patches* tão logo quanto possível. Portanto, um *patch* pode não abordar o problema adequadamente e pode causar efeitos colaterais negativos. Também, em alguns casos, a desinstalação de um *patch* pode não ser facilmente realizável após sua instalação.

Quando testes adequados de *patch* não forem possíveis, por exemplo, devido a custos ou falta de recursos, um atraso no uso do *patch* pode ser considerado para avaliar os riscos associados, baseado nas experiências relatadas por outros usuários.

13 Gestão de incidentes de segurança da informação

13.1 Notificação de fragilidades e eventos de segurança da informação

Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Convém que sejam estabelecidos procedimentos formais de registro e escalonamento. Convém que todos os funcionários, fornecedores e terceiros estejam conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança dos ativos da organização. Convém que seja requerido que os eventos de segurança da informação e fragilidades sejam notificados, tão logo quanto possível, ao ponto de contato designado.

13.1.1 Notificação de eventos de segurança da informação

Controle
Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

Diretrizes para Implementação
Convém que um procedimento de notificação formal seja estabelecido para relatar os eventos de segurança da informação, junto com um procedimento de resposta a incidente e escalonamento, estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação. Convém que um ponto de contato seja estabelecido para receber as notificações dos eventos de segurança da informação. Convém que este ponto de contato seja de conhecimento de toda a organização e esteja sempre disponível e em condições de assegurar uma resposta adequada e oportuna.

Convém que todos os funcionários, fornecedores e terceiros sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato designado para este fim. Convém que os procedimentos incluam:

a) processos adequados de realimentação para assegurar que os eventos de segurança da informação relatados sejam notificados dos resultados após a questão ter sido conduzida e concluída;

b) formulário para apoiar a ação de notificar um evento de segurança da informação e ajudar as pessoas a lembrar as ações necessárias para a notificação do evento;

c) o comportamento correto a ser tomado no caso de um evento de segurança da informação, como, por exemplo:

   1) anotar todos os detalhes importantes imediatamente (por exemplo, tipo de não-conformidade ou violação, mau funcionamento, mensagens na tela, comportamento estranho);

   2) não tomar nenhuma ação própria, mas informar imediatamente o evento ao ponto de contato;

d) referência para um processo disciplinar formal estabelecido para lidar com funcionários, fornecedores ou terceiros que cometam violações de segurança da informação.

Em ambientes de alto risco, podem ser fornecidos alarmes de coação[4] através do qual a pessoa que está sendo coagida possa sinalizar o que está ocorrendo. Convém que os procedimentos para responder a alarmes de coação reflitam o alto risco que a situação exige.

---

[4] Alarme de coação é um método usado para indicar, de forma secreta, que uma ação está acontecendo sob coação.

Informações adicionais
Exemplos de eventos e incidentes de segurança da informação são:

a) perda de serviço, equipamento ou recursos;

b) mau funcionamento ou sobrecarga de sistema;

c) erros humanos;

d) não-conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) mudanças descontroladas de sistemas;

g) mau funcionamento de *software* ou *hardware*;

h) violação de acesso.

Considerando os cuidados com os aspectos de confidencialidade, os incidentes de segurança da informação podem ser utilizados em treinamento de conscientização (ver 8.2.2) como exemplos do que poderia ocorrer, como responder a tais incidentes e como evitá-los futuramente. Para ser capaz de destinar os eventos e incidentes de segurança da informação adequadamente, pode ser necessário coletar evidências tão logo quanto possível depois da ocorrência (ver 13.2.3).

Um mau funcionamento ou outras anomalias de comportamento de sistemas podem ser um indicador de um ataque de segurança ou violação de segurança e, portanto, convém que sempre sejam notificados como um evento de segurança da informação.

Mais informações sobre notificação de eventos de segurança da informação e gestão de incidentes de segurança da informação podem ser encontradas na ISO/IEC TR 18044.

13.1.2 Notificando fragilidades de segurança da informação

Controle
Convém que os funcionários, fornecedores e terceiros de sistemas e serviços de informação sejam instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.

Diretrizes para implementação
Convém que os funcionários, fornecedores e terceiros notifiquem esse assunto o mais rápido possível para sua direção ou diretamente ao seu provedor de serviços, de forma a prevenir incidentes de segurança da informação. Convém que o mecanismo de notificação seja fácil, acessível e disponível sempre que possível. Convém que os usuários sejam informados que não podem, sob nenhuma circunstância, tentar averiguar fragilidade suspeita.

Informações adicionais
Convém que os funcionários, fornecedores e terceiros sejam alertados para não tentarem averiguar uma fragilidade de segurança da informação suspeita. Testar fragilidades pode ser interpretado como um uso impróprio potencial do sistema e também pode causar danos ao sistema ou serviço de informação, resultando em responsabilidade legal ao indivíduo que efetuar o teste.

13.2 Gestão de incidentes de segurança da informação e melhorias

Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

Convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados. Convém que um processo de melhoria contínua seja aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

Convém que onde evidências sejam exigidas, estas sejam coletadas para assegurar a conformidade com as exigências legais.

13.2.1 Responsabilidades e procedimentos

Controle
Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Diretrizes para implementação
Convém que, adicionalmente à notificação de eventos de segurança da informação e fragilidades (ver 13.1), o monitoramento de sistemas, alertas e vulnerabilidades (10.10.2) seja utilizado para a detecção de incidentes de segurança da informação. Convém que as seguintes diretrizes para procedimentos de gestão de incidentes de segurança da informação sejam consideradas:

a) procedimentos sejam estabelecidos para manusear diferentes tipos de incidentes de segurança da informação, incluindo:

   1) falhas de sistemas de informações e perda de serviços;

   2) código malicioso (ver 10.4.1);

   3) *denial of service* (negação de serviço);

   4) erros resultantes de dados incompletos ou inconsistentes;

   5) violações de confidencialidade e integridade;

   6) uso impróprio de sistemas de informação;

b) além dos planos de contingência (ver 14.1.3), convém que os procedimentos também considerem (ver 13.2.2):

   1) análise e identificação da causa do incidente;

   2) retenção;

   3) planejamento e implementação de ação corretiva para prevenir a sua repetição, se necessário;

   4) comunicação com aqueles afetados ou envolvidos com a recuperação do incidente;

   5) notificação da ação para a autoridade apropriada;

c) convém que trilhas de auditoria e evidências similares sejam coletadas (ver 13.2.3) e protegidas, como apropriado, para:

   1) análise de problemas internos;

   2) uso como evidência forense para o caso de uma potencial violação de contrato ou de normas reguladoras ou em caso de delitos civis ou criminais, por exemplo relacionados ao uso impróprio de computadores ou legislação de proteção dos dados;

   3) negociação para compensação ou ressarcimento por parte de fornecedores de *software* e serviços;

d) convém que as ações para recuperação de violações de segurança e correção de falhas do sistema sejam cuidadosa e formalmente controladas; convém que os procedimentos assegurem que:

   1) apenas funcionários explicitamente identificados e autorizados estejam liberados para acessar sistemas e dados em produção (ver 6.2 para acesso externo);

   2) todas as ações de emergência sejam documentadas em detalhe;

   3) as ações de emergência sejam relatadas para a direção e analisadas criticamente de maneira ordenada;

   4) a integridade dos sistemas do negócio e seus controles sejam validados na maior brevidade.

Convém que os objetivos da gestão de incidentes de segurança da informação estejam em concordância com a direção e que seja assegurado que os responsáveis pela gestão de incidentes de segurança da informação entendem as prioridades da organização no manuseio de incidentes de segurança da informação.

Informações adicionais
Os incidentes de segurança da informação podem transcender fronteiras organizacionais e nacionais. Para responder a estes incidentes, cada vez mais há a necessidade de resposta coordenada e troca de informações sobre eles com organizações externas, quando apropriado.

13.2.2 Aprendendo com os incidentes de segurança da informação

Controle
Convém que sejam estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.

Diretrizes para implementação
Convém que a informação resultante da análise de incidentes de segurança da informação seja usada para identificar incidentes recorrentes ou de alto impacto.

Informações adicionais
A análise de incidentes de segurança da informação pode indicar a necessidade de melhorias ou controles adicionais para limitar a freqüência, danos e custos de ocorrências futuras ou para ser levada em conta quando for realizado o processo de análise crítica da política de segurança da informação (ver 5.1.2).

13.2.3 Coleta de evidências

Controle
Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição(ões) pertinente(s).

Diretrizes para implementação
Convém que procedimentos internos sejam elaborados e respeitados para as atividades de coleta e apresentação de evidências com o propósito de ação disciplinar movida em uma organização.

Em geral, as normas para evidências abrangem:

a) admissibilidade da evidência: se a evidência pode ser ou não utilizada na corte;

b) importância da evidência: qualidade e inteireza da evidência.

Para obter a admissibilidade da evidência, convém que a organização assegure que seus sistemas de informação estejam de acordo com qualquer norma ou código de prática publicado para produção de evidência admissível.

Convém que o valor da evidência esteja de acordo com algum requisito aplicável. Para obter o valor da evidência, convém que a qualidade e a inteireza dos controles usados para proteger as evidências de forma correta e consistente (ou seja, o processo de controle de evidências) durante todo o período de armazenamento e processamento da evidência sejam demonstradas por uma trilha forte de evidência. Em geral, essa trilha forte de evidência pode ser estabelecida sob as seguintes condições:

a) para documentos em papel: o original é mantido de forma segura, com um registro da pessoa que o encontrou, do local e data em que foi encontrado e quem testemunhou a descoberta; convém que qualquer investigação assegure que os originais não foram adulterados;

b) para informação em mídia eletrônica: convém que imagens espelho ou cópias (dependendo de requisitos aplicáveis) de quaisquer mídias removíveis, discos rígidos ou em memórias sejam providenciadas para assegurar disponibilidade; convém que o registro de todas as ações tomadas durante o processo de cópia seja guardado e que o processo seja testemunhado; convém que a mídia original que contém a informação e o registro (ou, caso isso não seja possível, pelo menos uma imagem espelho ou cópia) seja mantido de forma segura e intocável.

Convém que qualquer trabalho forense seja somente realizado em cópias do material de evidência. Convém que a integridade de todo material de evidência seja preservada. Convém que o processo de cópia de todo material de evidência seja supervisionado por pessoas confiáveis e que as informações sobre a data, local, pessoas, ferramentas e programas envolvidos no processo de cópia sejam registradas.

Informações adicionais
Quando um evento de segurança da informação é detectado, pode não ser óbvio que ele resultará num possível processo jurídico. Entretanto, existe o perigo de que a evidência seja destruída intencional ou acidentalmente antes que seja percebida a seriedade do incidente. É conveniente envolver um advogado ou a polícia tão logo seja constatada a possibilidade de processo jurídico e obter consultoria sobre as evidências necessárias.

As evidências podem ultrapassar limites organizacionais e/ou de jurisdições. Nesses casos, convém assegurar que a organização seja devidamente autorizada para coletar as informações requeridas como evidências. Convém que os requisitos de diferentes jurisdições sejam também considerados para maximizar as possibilidades de admissão da evidência em todas as jurisdições relevantes.

14 Gestão da continuidade do negócio

14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

Convém que o processo de gestão da continuidade do negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação. Convém que este processo identifique os processos críticos e integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativo a tais aspectos como operações, funcionários, materiais, transporte e instalações.

Convém que as conseqüências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços estejam sujeitas a uma análise de impacto nos negócios. Convém que os planos de continuidade do negócio sejam desenvolvidos e implementados para assegurar que as operações essenciais sejam recuperadas dentro da requerida escala de tempo. Convém que a segurança da informação seja uma parte integrante do processo global de continuidade de negócios e a gestão de outros processos dentro da organização.

Convém que a gestão da continuidade do negócio inclua controles para identificar e reduzir riscos, em complementação ao processo de análise/avaliação de riscos global, limite as conseqüências aos danos do incidente e garanta que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio

Controle
Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.

Diretrizes para implementação
Convém que este processo agregue os seguintes elementos-chave da gestão da continuidade do negócio:

a) entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, incluindo a identificação e priorização dos processos críticos do negócio (ver 14.1.2);

b) identificação de todos os ativos envolvidos em processos críticos de negócio (ver 7.1.1);

c) entendimento do impacto que incidentes de segurança da informação provavelmente terão sobre os negócios (é importante que as soluções encontradas possam tratar tanto os pequenos incidentes, como os mais sérios, que poderiam colocar em risco a continuidade da organização) e estabelecimento dos objetivos do negócio dos recursos de processamento da informação;

d) consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade do negócio, bem como a parte de gestão de risco operacional;

e) identificação e consideração da implementação de controles preventivos e de mitigação;

f) identificação de recursos financeiros, organizacionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação;

g) garantia da segurança de pessoal e proteção de recursos de processamento das informações e bens organizacionais;

h) detalhamento e documentação de planos de continuidade de negócio que contemplem os requisitos de segurança da informação alinhados com a estratégia da continuidade do negócio estabelecida (ver 14.1.3);

i) testes e atualizações regulares dos planos e processos implantados (ver 14.1.5);

j) garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização. Convém que a responsabilidade pela coordenação do processo de gestão de continuidade de negócios seja atribuída a um nível adequado dentro da organização (ver 6.1.1).

14.1.2 Continuidade de negócios e análise/avaliação de riscos

Controle
Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as conseqüências para a segurança de informação.

Diretrizes para implementação
Convém que os aspectos da continuidade do negócios relativos à segurança da informação sejam baseados na identificação de eventos (ou sucessão de eventos) que possam causar interrupções aos processos de negócios das organizações, por exemplo, falha de equipamento, erros humanos, furto ou roubo, incêndio, desastres naturais e atos terroristas. Em seguida, convém que seja feita uma análise/avaliação de riscos para a determinação da probabilidade e impacto de tais interrupções, tanto em termos de escala de dano quanto em relação ao período de recuperação.

Convém que as análises/avaliações de riscos da continuidade do negócio sejam realizadas com total envolvimento dos responsáveis pelos processos e recursos do negócio. Convém que a análise/avaliação considere todos os processos do negócio e não esteja limitada aos recursos de processamento das informações, mas inclua os resultados específicos da segurança da informação. É importante a junção de aspectos de riscos diferentes, para obter um quadro completo dos requisitos de continuidade de negócios da organização. Convém que a análise/avaliação identifique, quantifique e priorize os critérios baseados nos riscos e os objetivos pertinentes à organização, incluindo recursos críticos, impactos de interrupção, possibilidade de ausência de tempo e prioridades de recuperação.

Em função dos resultados da análise/avaliação de riscos, convém que um plano estratégico seja desenvolvido para se determinar a abordagem mais abrangente a ser adotada para a continuidade dos negócios. Uma vez criada a estratégia, convém que ela seja validada pela direção e que um plano seja elaborado e validado para implementar tal estratégia.

14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Controle

Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

Diretrizes para implementação

Convém que o processo de planejamento da continuidade de negócios considere os seguintes itens:

a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;

b) identificação da perda aceitável de informações e serviços;

c) implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários; atenção especial precisa ser dada à avaliação de dependências externas ao negócio e de contratos existentes;

d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;

e) documentação dos processos e procedimentos acordados;

f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;

g) teste e atualização dos planos.

Convém que o processo de planejamento foque os objetivos requeridos do negócio, por exemplo recuperação de determinados serviços específicos para os clientes, em um período de tempo aceitável. Convém identificar os serviços e recursos que facilitam isso, prevendo a contemplação de pessoal e recursos em geral, além da tecnologia de informação, assim como o procedimento de recuperação dos recursos de processamento das informações. Tais procedimentos de recuperação podem incluir procedimentos com terceiros na forma de um acordo de reciprocidade, ou um contrato de prestação de serviços.

Convém que o plano de continuidade do negócio trate as vulnerabilidades da organização, que pode conter informações sensíveis e que necessitem de proteção adequada. Convém que cópias do plano de continuidade do negócio sejam guardadas em um ambiente remoto, a uma distância suficiente para escapar de qualquer dano de um desastre no local principal. Convém que o gestor garanta que as cópias dos planos de continuidade do negócio estejam atualizadas e protegidas no mesmo nível de segurança como aplicado no ambiente principal. Convém que outros materiais necessários para a execução do plano de continuidade do negócio também sejam armazenados em local remoto.

Convém que, se os ambientes alternativos temporários forem usados, o nível de controles de segurança implementados nestes locais seja equivalente ao ambiente principal.

Informações adicionais
Convém que seja destacado que as atividades e os planos de gerenciamento de crise (ver 14.1.3 f)) possam ser diferentes de gestão de continuidade de negócios, isto é, uma crise pode acontecer e ser suprida através dos procedimentos normais de gestão.

14.1.4 Estrutura do plano de continuidade do negócio

Controle
Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

Diretrizes para implementação
Convém que cada plano de continuidade do negócio descreva o enfoque para continuidade, por exemplo, o enfoque para assegurar a disponibilidade e segurança do sistema de informação ou da informação. Convém que cada plano também especifique o plano de escalonamento e as condições para sua ativação, assim como as responsabilidades individuais para execução de cada uma das atividades do plano. Quando novos requisitos são identificados, é importante que os procedimentos de emergência relacionados sejam ajustados de forma apropriada, por exemplo o plano de abandono ou o procedimento de recuperação. Convém que os procedimentos do programa de gestão de mudança da organização sejam incluídos para assegurar que os assuntos de continuidade de negócios estejam sempre direcionados adequadamente.

Convém que cada plano tenha um gestor específico. Convém que procedimentos de emergência, de recuperação, manual de planejamento e planos de reativação sejam de responsabilidade dos gestores dos recursos de negócios ou dos processos envolvidos. Convém que procedimentos de recuperação para serviços técnicos alternativos, como processamento de informação e meios de comunicação, sejam normalmente de responsabilidade dos provedores de serviços.

Convém que uma estrutura de planejamento para continuidade de negócios contemple os requisitos de segurança da informação identificados e considere os seguintes itens:

a) condições para ativação dos planos, os quais descrevem os processos a serem seguidos (como se avaliar a situação, quem deve ser acionado etc.) antes de cada plano ser ativado;

b) procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio;

c) procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infra-estrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário;

d) procedimentos operacionais temporários para seguir durante a conclusão de recuperação e restauração;

e) procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações;

f) uma programação de manutenção que especifique quando e como o plano deverá ser testado e a forma de se proceder à manutenção deste plano;

g) atividades de treinamento, conscientização e educação com o propósito de criar o entendimento do processo de continuidade de negócios e de assegurar que os processos continuem a ser efetivo;

h) designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano. Convém que suplentes sejam definidos quando necessário;

i) os ativos e recursos críticos precisam estar aptos a desempenhar os procedimentos de emergência, recuperação e reativação.

14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio

Controle
Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Diretrizes para implementação
Convém que os testes do plano de continuidade do negócio assegurem que todos os membros da equipe de recuperação e outras pessoas relevantes estejam conscientes dos planos e de suas responsabilidades para a continuidade do negócio e a segurança da informação, e conheçam as suas atividades quando um plano for acionado.

Convém que o planejamento e a programação dos testes do(s) plano(s) de continuidade de negócios indiquem como e quando cada elemento do plano seja testado. Convém que os componentes isolados do(s) plano(s) sejam freqüentemente testados.

Convém que várias técnicas sejam utilizadas, de modo a assegurar a confiança de que o(s) plano(s) irá(ão) operar consistentemente em casos reais. Convém que sejam considerados:

a) testes de mesa simulando diferentes cenários (verbalizando os procedimentos de recuperação para diferentes formas de interrupção);

b) simulações (particularmente útil para o treinamento do pessoal nas suas atividades gerenciais após o incidente);

c) testes de recuperação técnica (garantindo que os sistemas de informação possam ser efetivamente recuperados);

d) testes de recuperação em um local alternativo (executando os processos de negócios em paralelo com a recuperação das operações distantes do local principal);

e) testes dos recursos, serviços e instalações de fornecedores (assegurando que os serviços e produtos fornecidos por terceiros atendem aos requisitos contratados);

f) ensaio geral (testando se a organização, o pessoal, os equipamentos, os recursos e os processos podem enfrentar interrupções).

Estas técnicas podem ser utilizadas por qualquer organização. Convém que elas reflitam a natureza do plano de recuperação específico. Convém que os resultados dos testes sejam registrados e ações tomadas para a melhoria dos planos, onde necessário.

Convém que a responsabilidade pelas análises críticas periódicas de cada parte do plano seja definida e estabelecida. Convém que a identificação de mudanças nas atividades do negócio que ainda não tenham sido contempladas nos planos de continuidade de negócio seja seguida por uma apropriada atualização do plano. Convém que um controle formal de mudanças assegure que os planos atualizados são distribuídos e reforçados por análises críticas periódicas do plano como um todo.

Os exemplos de mudanças onde convém que a atualização dos planos de continuidade do negócio seja considerada são a aquisição de novos equipamentos, atualização de sistemas e mudanças de:

a) pessoal;

b) endereços ou números telefônicos;

c) estratégia de negócio;

d) localização, instalações e recursos;

e) legislação;

f) prestadores de serviços, fornecedores e clientes-chave;

g) processos (inclusões e exclusões);

h) risco (operacional e financeiro).

15 Conformidade

15.1 Conformidade com requisitos legais

Objetivo: Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários.

Convém que consultoria em requisitos legais específicos seja procurada em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais. Os requisitos legislativos variam de país para país e também para a informação criada em um país e transmitida para outro (isto é, fluxo de dados transfronteira).

15.1.1 Identificação da legislação aplicável

Controle
Convém que todos os requisitos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização

Diretrizes para implementação
Convém que os controles específicos e as responsabilidades individuais para atender a estes requisitos sejam definidos e documentados de forma similar.

15.1.2 Direitos de propriedade intelectual

Controle
Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.

Diretrizes para implementação
Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

a) divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de *software* e de informação;

b) adquirir *software* somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não está sendo violado;

c) manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

d) manter de forma adequada os registros de ativos e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

e) manter provas e evidências da propriedade de licenças, discos-mestre, manuais etc.;

f) implementar controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas;

g) conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam instalados;

h) estabelecer uma política para a manutenção das condições adequadas de licenças;

i) estabelecer uma política para disposição ou transferência de *software* para outros;

j) utilizar ferramentas de auditoria apropriadas;

k) cumprir termos e condições para *software* e informação obtidos a partir de redes públicas;

l) não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;

m) não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Informações adicionais
Direitos de propriedade intelectual incluem direitos de *software* ou documento, direitos de projeto, marcas, patentes e licenças de códigos-fonte.

Produtos de *software* proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença, por exemplo, restringe o uso dos produtos em máquinas especificadas ou limita a cópia apenas para criação de uma cópia de segurança. A questão relativa aos direitos de propriedade intelectual de *software* desenvolvido pela organização precisa ser esclarecida com as pessoas.

Legislação, regulamentação e requisitos contratuais podem estabelecer restrições para cópia de material que tenha direitos autorais. Em particular, pode ser requerido que somente material que seja desenvolvido pela organização ou que foi licenciado ou fornecido pelos desenvolvedores para a organização seja utilizado. Violações aos direitos de propriedade intelectual podem conduzir a ações legais, que podem envolver processos criminais.

15.1.3 Proteção de registros organizacionais

Controle
Convém que registros importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

Diretrizes para implementação
Convém que registros sejam categorizados em tipos de registros, tais como registros contábeis, registros de base de dados, registros de transações, registros de auditoria e procedimentos operacionais, cada qual com detalhes do período de retenção e do tipo de mídia de armazenamento, como, por exemplo, papel, microficha, meio magnético ou ótico. Convém que quaisquer chaves de criptografia relacionadas com arquivos cifrados ou assinaturas digitais (ver 12.3) sejam também armazenadas para permitir a decifração de registros pelo período de tempo que os registros são mantidos.

Convém que cuidados sejam tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros. Convém que os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações dos fabricantes. Convém que, para o armazenamento de longo tempo, o uso de papel e microficha seja considerado.

Onde mídias eletrônicas armazenadas forem escolhidas, convém que sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados (leitura tanto na mídia como no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia.

Convém que sistemas de armazenamento de dados sejam escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável, dependendo dos requisitos a serem atendidos.

Convém que o sistema de armazenamento e manuseio assegure a clara identificação dos registros e dos seus períodos de retenção, conforme definido pela legislação nacional ou regional ou por regulamentações, se aplicável. Convém que seja permitida a destruição apropriada dos registros após esse período, caso não sejam mais necessários à organização.

Para atender aos objetivos de proteção dos registros, convém que os seguintes passos sejam tomados dentro da organização:

a) emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

b) elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido;

c) manter um inventário das fontes de informações-chave;

d) implementar controles apropriados para proteger registros e informações contra perda, destruição e falsificação.

Informações adicionais
Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, contratuais ou regulamentares, assim como para apoiar as atividades essenciais do negócio. Exemplo disso são os registros que podem ser exigidos como evidência de que uma organização opera de acordo com as regras estatutárias e regulamentares, para assegurar a defesa adequada contra potenciais processos civis ou criminais ou confirmar a situação financeira de uma organização perante os acionistas, partes externas e auditores. O período de tempo e o conteúdo da informação retida podem estar definidos através de leis ou regulamentações nacionais.

Outras informações sobre como gerenciar os registros organizacionais, podem ser encontradas na ISO 15489-1.

15.1.4 Proteção de dados e privacidade de informações pessoais

Controle
Convém que a privacidade e a proteção de dados sejam asseguradas conforme exigido nas legislações, regulamentações e, se aplicável, nas cláusulas contratuais pertinentes.

Diretrizes para implementação
Convém que uma política de privacidade e proteção de dados da organização seja desenvolvida e implementada. Convém que esta política seja comunicada a todas as pessoas envolvidas no processamento de informações pessoais.

A conformidade com esta política e todas as legislações e regulamentações relevantes de proteção de dados necessita de uma estrutura de gestão e de controles apropriados. Geralmente isto é melhor alcançado através de uma pessoa responsável, como, por exemplo, um gestor de proteção de dados, que deve fornecer orientações gerais para gerentes, usuários e provedores de serviço sobre as responsabilidades de cada um e sobre quais procedimentos específicos recomenda-se seguir. Convém que a responsabilidade pelo tratamento das informações pessoais e a garantia da conscientização dos princípios de proteção dos dados sejam tratadas de acordo com as legislações e regulamentações relevantes. Convém que medidas organizacionais e técnicas apropriadas para proteger as informações pessoais sejam implementadas.

Informações adicionais
Alguns países têm promulgado leis que estabelecem controles na coleta, no processamento e na transmissão de dados pessoais (geralmente informação sobre indivíduos vivos que podem ser identificados a partir de tais informações). Dependendo da respectiva legislação nacional, tais controles podem impor responsabilidades sobre aqueles que coletam, processam e disseminam informação pessoal, e podem restringir a capacidade de transferência desses dados para outros países.

15.1.5 Prevenção de mau uso de recursos de processamento da informação

Controle
Convém que os usuários sejam dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados.

Diretrizes para implementação:
Convém que a direção aprove o uso de recursos de processamento da informação. Convém que qualquer uso destes recursos para propósitos não relacionados ao negócio ou não autorizados, sem a aprovação da direção (ver 6.1.4), ou para quaisquer propósitos não autorizados, seja considerado como uso impróprio desses recursos. Se qualquer atividade não autorizada for identificada por processo de monitoração ou outros meios, convém que esta atividade seja levada ao conhecimento do gestor responsável para que sejam aplicadas as ações disciplinares e/ou legais pertinentes.

Convém que se busque uma assessoria legal antes da implementação dos procedimentos de monitoração.

Convém que todos os usuários estejam conscientes do escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado. Isto pode ser alcançado pelo registro das autorizações dos usuários por escrito, convém que a cópia seja assinada pelo usuário e armazenada de forma segura pela organização. Convém que os funcionários de uma organização, fornecedores e terceiros sejam informados de que nenhum acesso é permitido com exceção daqueles que foram autorizados.

No momento da conexão inicial, convém que seja apresentada uma mensagem de advertência para indicar que o recurso de processamento da informação que está sendo usado é de propriedade da organização e que não são permitidos acessos não autorizados. O usuário tem que confirmar e reagir adequadamente à mensagem na tela para continuar com o processo de conexão (ver 11.5.1).

Informações adicionais
Os recursos de processamento da informação de uma organização são destinados básica ou exclusivamente para atender aos propósitos do negócio.

Ferramentas do tipo detecção de intrusos, inspeção de conteúdo e outras formas de monitoração podem ajudar a prevenir e detectar o mau uso dos recursos de processamento da informação.

Muitos países têm legislação para proteger contra o mau uso do computador. Pode ser crime usar um computador para propósitos não autorizados.

A legalidade do processo de monitoração do uso do computador varia de país para país e pode requerer que a direção avise a todos os usuários dessa monitoração e/ou que concordem formalmente com este processo. Quando o sistema estiver sendo usado para acesso público (por exemplo, um servidor público *web*) e sujeito a uma monitoração de segurança, convém que uma mensagem seja exibida na tela informando deste processo.

15.1.6 Regulamentação de controles de criptografia

Controle
Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos e regulamentações pertinentes.

Diretrizes para implementação
Convém que os seguintes itens sejam considerados para conformidade com leis, acordos e regulamentações pertinentes:

a) restrições à importação e/ou exportação de *hardware* e *software* de computador para execução de funções criptográficas;

b) restrições à importação e/ou exportação de *hardware* e *software* de computador que foi projetado para ter funções criptográficas embutidas;

c) restrições no uso de criptografia;

d) métodos mandatários ou discricionários de acesso pelas autoridades dos países à informação cifrada por *hardware* ou *software* para fornecer confidencialidade ao conteúdo.

Convém que assessoria jurídica seja obtida para garantir a conformidade com as legislações e leis nacionais vigentes. Também convém que seja obtida assessoria jurídica antes de se transferirem informações cifradas ou controles de criptografia para outros países.

15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica

Objetivo: Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

Convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares.

Convém que tais análises críticas sejam executadas com base nas políticas de segurança da informação apropriadas e que as plataformas técnicas e sistemas de informação sejam auditados em conformidade com as normas de segurança da informação implementadas pertinentes e com os controles de segurança documentados.

15.2.1 Conformidade com as políticas e normas de segurança da informação

Controle
Convém que gestores garantam que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.

Diretrizes para implementação
Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade do processamento da informação dentro da sua área de responsabilidade com as políticas de segurança da informação, normas e quaisquer outros requisitos de segurança.

Se qualquer não-conformidade for encontrada como um resultado da análise crítica, convém que os gestores:

a) determinem as causas da não-conformidade;

b) avaliem a necessidade de ações para assegurar que a não-conformidade não se repita;

c) determinem e implementem ação corretiva apropriada;

d) analisem criticamente a ação corretiva tomada.

Convém que os resultados das análises críticas e das ações corretivas realizadas pelos gestores sejam registrados e que esses registros sejam mantidos. Convém que os gestores relatem os resultados para as pessoas que estão realizando a análise crítica independente (ver 6.1.8), quando a análise crítica independente for realizada na área de sua responsabilidade.

Informações adicionais
A monitoração operacional de sistemas em uso é apresentada em 10.10.

15.2.2 Verificação da conformidade técnica

Controle
Convém que sistemas de informação sejam periodicamente verificados em sua conformidade com as normas de segurança da informação implementadas.

Diretrizes para implementação
Convém que a verificação de conformidade técnica seja executada manualmente (auxiliada por ferramentas de *software* apropriadas, se necessário) por um engenheiro de sistemas experiente, e/ou com a assistência de ferramentas automatizadas que gerem relatório técnico para interpretação subseqüente por um técnico especialista.

Se o teste de invasão ou avaliações de vulnerabilidades forem usados, convém que sejam tomadas precauções, uma vez que tais atividades podem conduzir a um comprometimento da segurança do sistema. Convém que tais testes sejam planejados, documentados e repetidos.

Convém que qualquer verificação de conformidade técnica somente seja executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas.

Informações adicionais
A verificação da conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de *hardware* e *software* foram corretamente implementados. Este tipo de verificação de conformidade requer a assistência de técnicos especializados.

A verificação de conformidade também engloba, por exemplo, testes de invasão e avaliações de vulnerabilidades, que podem ser executados por especialistas independentes contratados especificamente para este fim. Isto pode ser útil na detecção de vulnerabilidades do sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades.

Teste de invasão e avaliação de vulnerabilidades fornece um *snapshot* de um sistema em um estágio específico para um tempo específico. O *snapshot* está limitado para aquelas partes do sistema realmente testadas durante a etapa da invasão. O teste de invasão e as avaliações de vulnerabilidades não são um substituto da análise/avaliação de riscos.

15.3 Considerações quanto à auditoria de sistemas de informação

Objetivo: Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

Convém que existam controles para a proteção dos sistemas operacionais e ferramentas de auditoria durante as auditorias de sistema de informação.

Proteção também é necessária para proteger a integridade e prevenir o uso indevido das ferramentas de auditoria.

15.3.1 Controles de auditoria de sistemas de informação

Controle
Convém que requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio.

Diretrizes para implementação
Convém que as seguintes diretrizes sejam observadas:

a) requisitos de auditoria sejam acordados com o nível apropriado da administração;

b) escopo da verificação seja acordado e controlado;

c) a verificação esteja limitada ao acesso somente para leitura de *software* e dados;

d) outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, e sejam apagados ao final da auditoria, ou dada proteção apropriada quando existir uma obrigação para guardar tais arquivos como requisitos da documentação da auditoria;

e) recursos para execução da verificação sejam identificados explicitamente e tornados disponíveis;

f) requisitos para processamento adicional ou especial sejam identificados e acordados;

g) todo acesso seja monitorado e registrado de forma a produzir uma trilha de referência; convém que o uso de trilhas de referência (*time stamped*) seja considerado para os sistemas ou dados críticos;

h) todos os procedimentos, requisitos e responsabilidades sejam documentados;

i) as pessoas que executem a auditoria sejam independentes das atividades auditadas.

15.3.2 Proteção de ferramentas de auditoria de sistemas de informação

Controle
Convém que o acesso às ferramentas de auditoria de sistema de informação seja protegido, para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

Diretrizes para implementação
Convém que acessos às ferramentas de auditoria de sistemas de informação, por exemplo, *software* ou arquivos de dados, sejam separados de sistemas em desenvolvimento e em operação e não sejam mantidos em fitas de biblioteca ou áreas de usuários, a menos que seja dado um nível apropriado de proteção adicional.

Informações adicionais
Quando terceiros estão envolvidos em uma auditoria, existe um risco de mau uso de ferramentas de auditoria por esses terceiros e da informação que está sendo acessada por este terceiro. Controles, tais como em 6.2.1 (para avaliar os riscos) e 9.1.2 (para restringir o acesso físico), podem ser considerados para contemplar este risco, e convém que quaisquer conseqüências, tais como trocar imediatamente as senhas reveladas para os auditores, sejam tomadas.

Bibliografia

ABNT NBR ISO 10007:2005 – Sistemas de gestão da qualidade - Diretrizes para a gestão de configuração

ABNT NBR ISO 19011:2002 – Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental

ABNT NBR ISO/IEC 12207:1998 – Tecnologia de informação - Processos de ciclo de vida de software

ABNT ISO/IEC Guia 2:1998 – Normalização e atividades relacionadas – Vocabulário geral

ABNT ISO/IEC Guia 73:2005 – Gestão de riscos – Vocabulário – Recomendações para uso em normas

ISO 15489-1:2001 – Information and documentation – Records management – Part 1: General

ISO/IEC 9796-2:2002 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

ISO/IEC 9796-3:2000 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

ISO/IEC 11770-1:1996 – Information technology – Security techniques – Key management – Part 1: Framework

ISO/IEC 13335-1:2004 – Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

ISO/IEC 13888-1: 1997 – Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 14516:2002 – Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

ISO/IEC 14888-1:1998 – Information technology – Security techniques – Digital signatures with appendix – Part 1: General

ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

ISO/IEC 18028-4 – Information technology – Security techniques – IT Network security – Part 4: Securing remote access

ISO/IEC TR 13335-3:1998 – Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

ISO/IEC TR 18044 – Information technology – Security techniques – Information security incident

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002

OECD Guidelines for Cryptography Policy, 1997

Índice

A

C

I

L

M

N

O

P

R

S

T

U

V